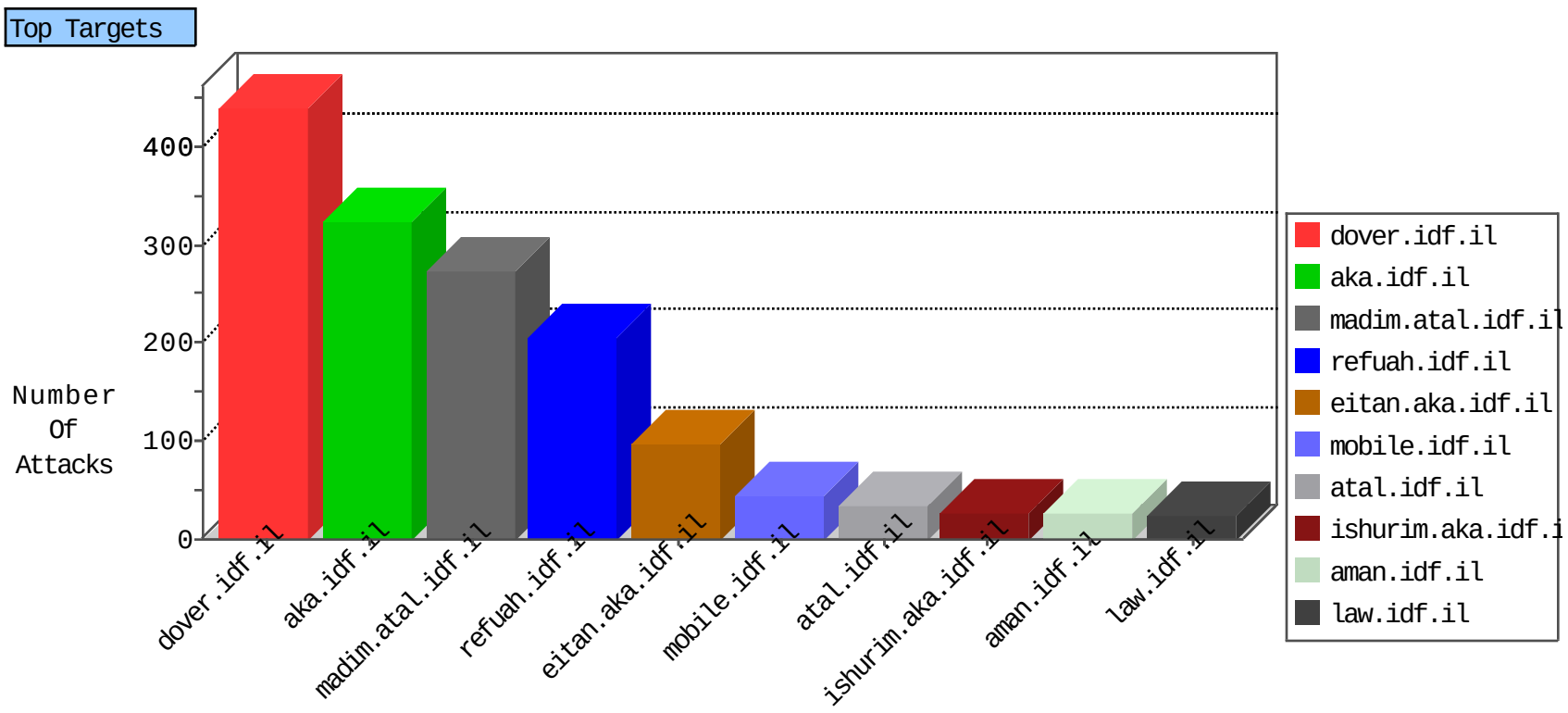
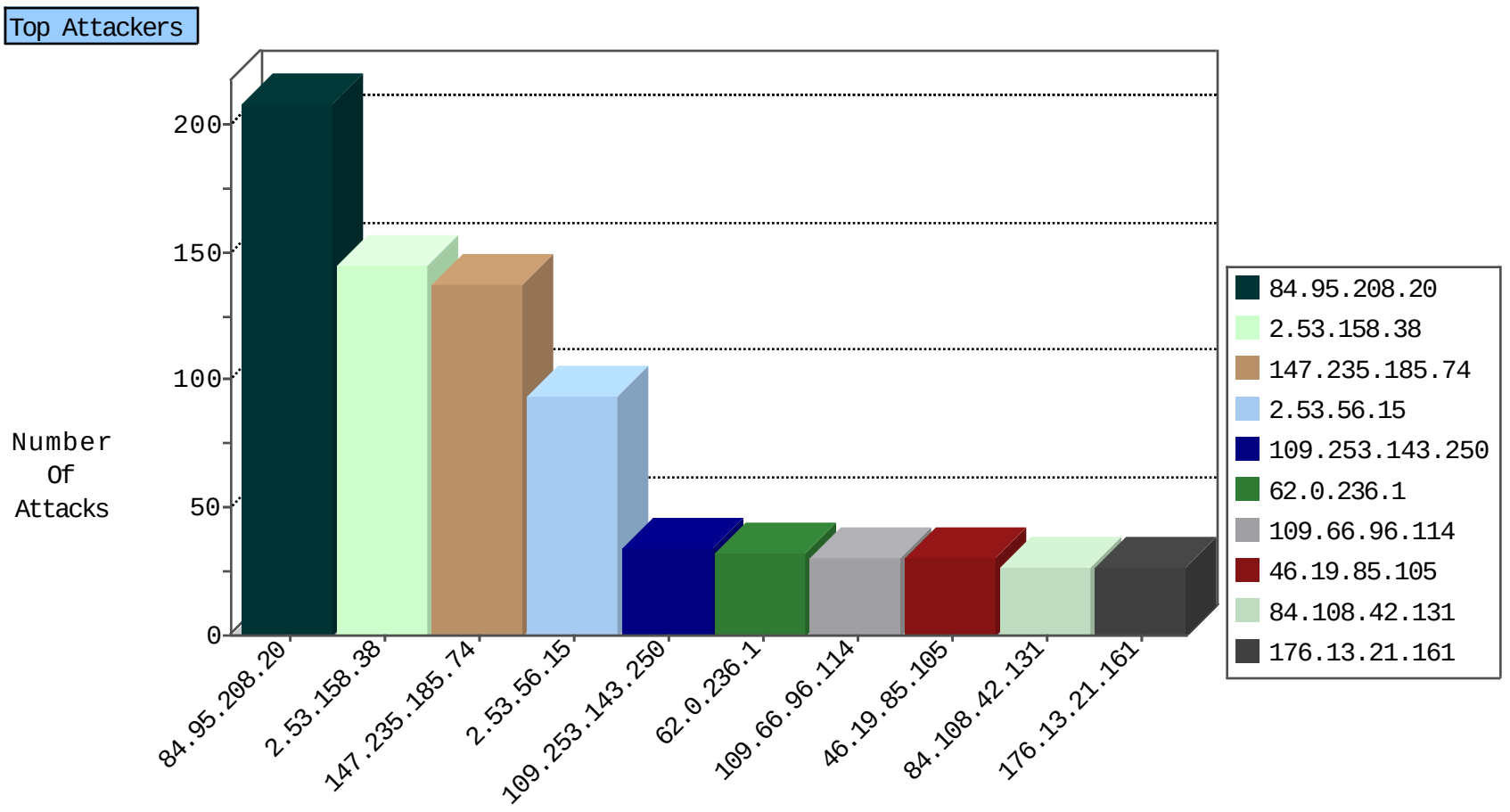
09-20-2016-12:04:04 to 09-20-2016-13:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-20-2016-12:04:04 to 09-20-2016-13:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.96.114	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
84.108.42.131	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
80.179.10.113	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
176.13.245.17	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
2.53.52.246	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
147.235.185.74	Israel	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
2.53.2.53	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
109.253.243.44	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
80.246.138.214	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
212.143.154.20	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
2.55.160.128	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
222.186.21.35	China	147.237.76.31	nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
68.180.229.223	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
195.62.53.168	Russian Federation	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	2
66.240.192.138	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
185.153.197.116		147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
80.179.222.227	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
185.153.197.116		147.237.76.44	e.refuah.idf.il	Black List	drop	1
64.137.175.102	Canada	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1

09-20-2016-12:04:04 to 09-20-2016-13:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-20-2016-12:04:04 to 09-20-2016-13:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.143.156.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.160.155	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.246.60	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
85.64.185.33	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.70.44.28	147.237.76.199	Hungary	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.93.158	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.6.226	147.237.77.74	Lithuania	law.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.85.19	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.71.146.48	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.213	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.2.28	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.185.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.135.15	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.220.82	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.248.160.155	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
212.116.72.226	147.237.77.19	Sweden	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
89.139.213.110	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
211.149.240.243	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
80.74.107.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.6.226	147.237.77.176	Lithuania	matpash.idf.il	ET SCAN Potential SSH Scan	1
62.90.144.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.6.64.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
147.236.28.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
119.92.233.197	147.237.76.86	Philippines	navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.53.146.112	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.119.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.61.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.60.153.178	147.237.72.167	Russian Federation	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1

09-20-2016-12:04:04 to 09-20-2016-13:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
147.235.185.74	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	98
147.235.185.74	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	35
62.0.236.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	31
62.0.235.160	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
195.60.235.58	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	17
62.0.200.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
62.0.197.85	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
62.0.237.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
85.64.159.213	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
207.241.229.68	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	13
46.19.85.105	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.86.149	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
212.199.218.246	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	10
2.53.158.68	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.76.203.100	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.22.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
2.53.22.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.85.19	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
212.126.121.186	Iraq	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	8
46.19.86.52	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.19	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.53	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
80.178.110.19	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.86.4	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.105	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.53.22.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
62.0.244.1	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.53	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
82.81.197.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
84.108.42.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.7	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.42.131	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
62.0.252.145	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.66.96.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.21.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.66.6	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.231.49	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.96.114	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
80.178.198.75	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.21.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
80.178.110.19	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
176.13.21.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.4	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
176.13.21.161	Israel	147.237.72.166	aka.idf.il	SYN Attack		monitor	5
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5

09-20-2016-12:04:04 to 09-20-2016-13:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.158.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	129
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	100
2.53.56.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	93
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	85
109.253.143.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
2.53.158.38	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	16
37.26.146.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
192.118.12.102	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.118.12.102	Block	7
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	6
10.102.70.28		147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
87.70.3.146	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
109.253.146.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.82	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
176.13.237.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.181.141.150	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
176.13.231.49	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
62.0.110.137	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/	Block	2
62.90.35.105	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.19.85.101	Israel	147.237.76.42	refuah.idf.il	Distributed Malformed URL	Block	1
212.199.103.82	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
2.53.152.122	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
79.178.247.130	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/brothers/gallery/showpicture.asp	Block	1
46.19.86.249	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method e-il in URL	Block	1
80.246.140.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.146.251	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
203.2.218.131	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
2.53.36.87	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.113.8	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
89.187.220.58	Lebanon	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/login/	Block	1
66.102.9.30	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
46.19.85.101	Israel	147.237.76.42	refuah.idf.il	Distributed Unknown HTTP Request Method	Block	1
192.118.12.102	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
79.180.61.135	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
176.13.2.88	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.29.250.225	Sweden	147.237.76.147	chinuch.aka.idf.il	Distributed PHP Attempt	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	1
37.142.250.230	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
209.95.56.53	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/giyus/login/	Block	1
176.13.247.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
77.138.160.140	France	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
94.188.139.68	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar	Block	1
66.228.41.233	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/pratim/pirteyerua/	Block	1
46.19.86.52	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in www.atal.idf.il/1437-he/atal.aspx	Block	1
192.118.12.102	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/sachar/scriptresource.axd	None	1
66.249.79.131	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.tech.atal.idf.il/templates/faq/faq.aspx	Block	1

09-20-2016-12:04:04 to 09-20-2016-13:04:04