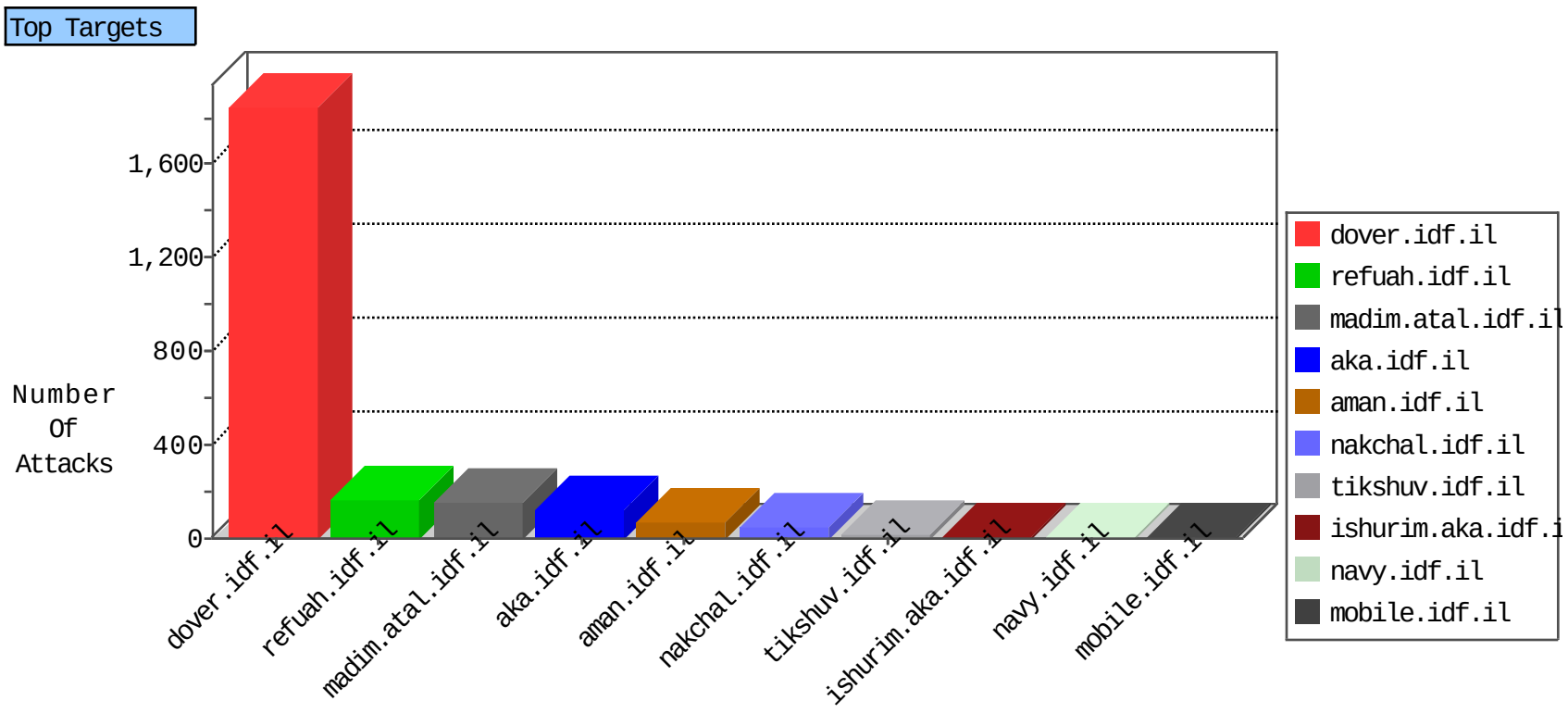
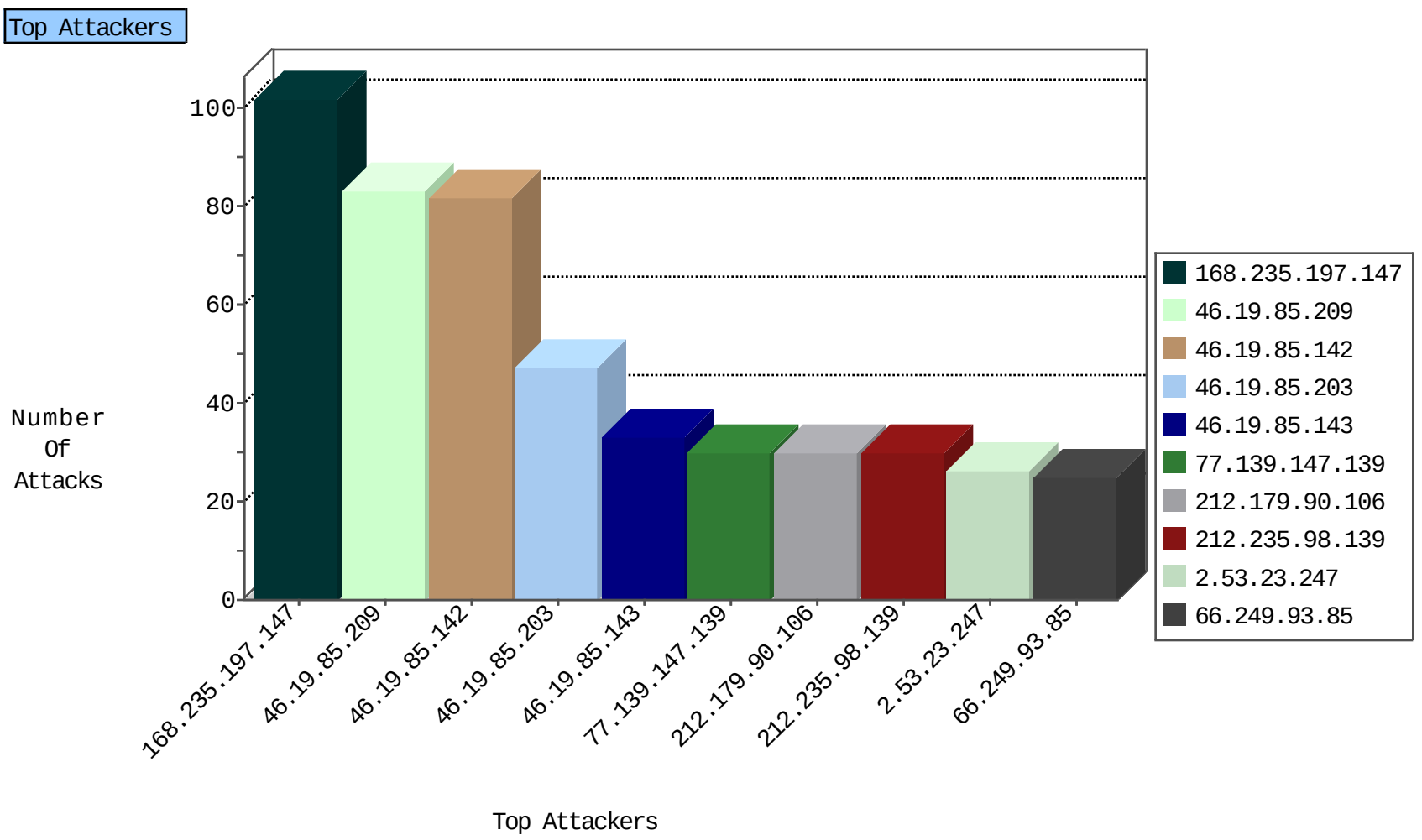
09-20-2016-14:04:01 to 09-20-2016-15:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-20-2016-14:04:01 to 09-20-2016-15:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
168.235.197.147	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
79.177.151.20	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
79.180.173.192	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
79.176.24.31	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
142.54.174.84	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
173.208.150.118	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
168.235.197.147	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
173.208.197.203	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
173.208.197.206	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
63.141.242.197	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1
207.46.13.155	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
142.54.174.85	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
69.30.193.254	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1
173.208.150.118	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
84.111.2.13	Israel	147.237.72.156	aman.idf.il	Black List	drop	1
63.141.242.197	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1

09-20-2016-14:04:01 to 09-20-2016-15:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
71.6.146.185	United States	147.237.0.16	my-kosher-kravi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
210.212.230.170	India	147.237.77.176	matpash.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1

09-20-2016-14:04:01 to 09-20-2016-15:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
170.149.168.65	147.237.77.74	United States	law.idf.il	Tehila - Perl LWP with fake user agent	2
77.127.35.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
138.99.12.34	147.237.77.234	Brazil	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
84.245.14.50	147.237.8.27	Netherlands	e.madim.atal.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
84.108.142.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.194.196.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.138.168	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
216.51.215.173	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.179.105.223	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.0.109.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.12.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.160.222.18	147.237.76.198	South Africa	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
2.55.10.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.76.34	Ukraine	yohalan.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
2.53.9.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.245.14.50	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.246.138.236	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.165.66.107	147.237.8.14	United Arab Emirates	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.125.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.54.168.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.172.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
139.162.13.205	147.237.0.34	Singapore	tikshuv.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
62.219.46.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.140.219	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.35	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
2.55.187.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -f -sS	1
2.53.153.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-20-2016-14:04:01 to 09-20-2016-15:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
168.235.197.147	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	94
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	30
46.19.85.209	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
66.249.93.83	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
46.19.85.203	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
66.249.93.85	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
46.19.85.143	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
31.210.187.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
46.19.85.209	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	22
192.118.36.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
66.249.93.87	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
62.0.197.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
89.139.147.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.19.86.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
37.26.149.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
141.226.218.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
141.0.13.88	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	15
46.19.85.203	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
141.226.218.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.47	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
77.139.147.139	France	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
185.24.207.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.53.181.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.209	Israel	147.237.76.31	nakchal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.209	Israel	147.237.76.31	nakchal.idf.i	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
109.160.179.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
2.53.60.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
89.139.160.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
85.64.99.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.181.251.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.31.47	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.176.24.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.150.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
62.0.221.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
100.92.149.35		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
77.125.51.255	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.177	Israel	147.237.76.31	nakchal.idf.i	Bad TCP sequence	Invalid ACK number	alert	8
46.19.86.177	Israel	147.237.76.31	nakchal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
2.53.15.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.55.4.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.116.24.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
199.203.94.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.15.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
109.253.131.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.138.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.142.9.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7

09-20-2016-14:04:01 to 09-20-2016-15:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
2.53.23.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
109.253.129.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
46.19.86.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
37.26.148.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
85.250.155.171	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	3
85.64.64.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.143.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.120.162.203	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
37.26.146.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.143.173.198	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.143.173.198	Block	2
109.253.192.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	2
37.142.191.84	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/images/	Block	2
85.250.155.171	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 85.250.155.171	Block	2
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Illegal Byte Code Character in Method cŸ¦}œ`Y,>MûÆ,•m[[#18]]•[[#26]]•'cl,Ù‰z*w©›Á•	Block	1
68.180.231.35	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
95.86.121.119	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
2.55.186.105	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.95.251.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
194.90.115.195	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/8/size338x0/1808.jpg	Block	1
77.139.70.52	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/112249.pdf	Block	1
52.16.137.212	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to /	Block	1
157.55.39.87	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
46.19.85.143	Israel	147.237.76.42	refuah.idf.il	Distributed Abnormally Long Request	Block	1
80.246.137.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Illegal Byte Code Character in URL	Block	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 77.126.240.205 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
46.19.86.139	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
77.139.192.18	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/yohalan/	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
157.55.39.156	United States	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	1
85.250.155.171	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
46.19.85.143	Israel	147.237.76.42	refuah.idf.il	Distributed Malformed URL	Block	1
81.218.37.2	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/send_but.png	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Unknown HTTP Request Method cŸ¦}œ`Y,>MûÆ,•m[[#18]]•[[#26]]•'cl,Ù‰z*w©›Á• in URL	Block	1
77.138.10.83	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.10.83	Block	1
46.19.86.218	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
78.46.42.235	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/brothers/skira/default.asp	Block	1
212.143.173.198	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/scrollpanetop.gif	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.106	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
87.69.213.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.143	Israel	147.237.76.42	refuah.idf.il	Distributed Unknown HTTP Request Method	Block	1
84.95.251.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
176.13.230.174	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.138.10.83	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/drushim	Block	1
46.117.197.156	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
139.162.13.205	Singapore	147.237.0.34	tikshuv.idf.il	Multiple Untraceable SSL Sessions from 139.162.13.205 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1

09-20-2016-14:04:01 to 09-20-2016-15:04:01