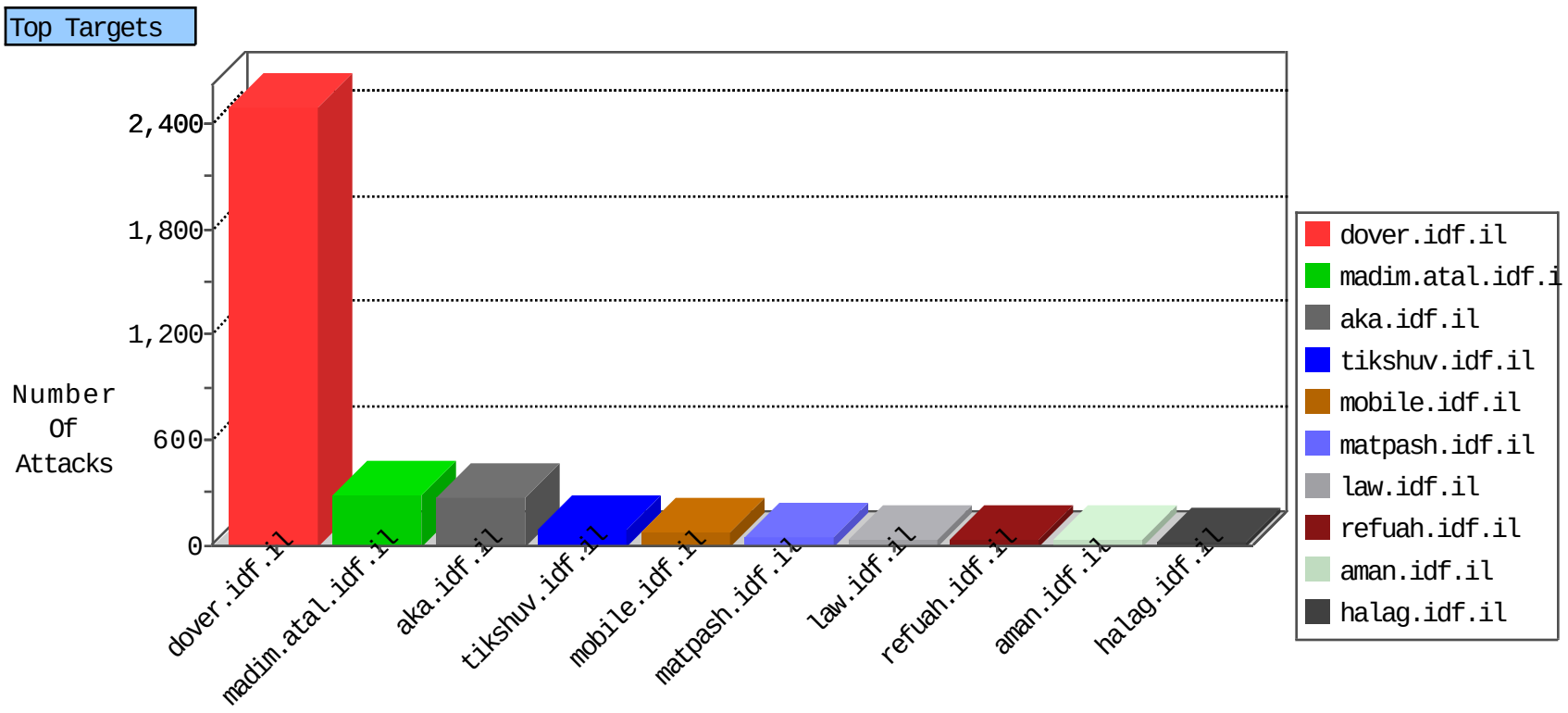
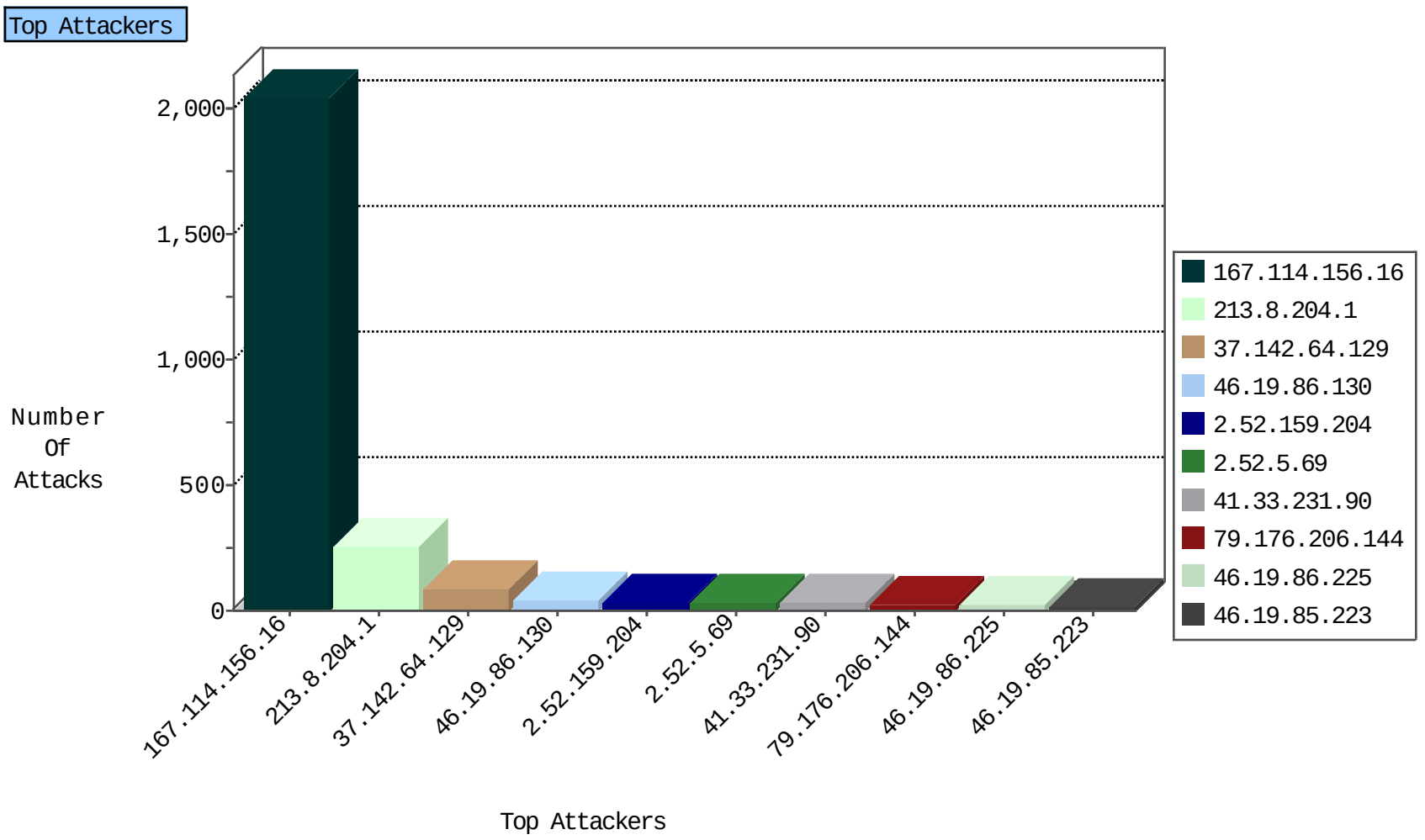
01-20-2016-20:04:01 to 01-20-2016-21:04:01

IDF Under Attack Daily Report





01-20-2016-20:04:01 to 01-20-2016-21:04:01

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	3065
66.249.93.107	Israel	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	8
109.67.168.125	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
66.249.81.212	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
119.126.201.215	China	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
151.80.230.89	Italy	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
66.249.93.184	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1

01-20-2016-20:04:01 to 01-20-2016-21:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
5.165.20.21	Russian Federation	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

01-20-2016-20:04:01 to 01-20-2016-21:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.111	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
41.13.136.157	147.237.77.216	South Africa	dover.idf.il	ET SCAN NMAP -sA (2)	2
213.8.204.1	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
66.249.79.75	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
168.62.238.153	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
5.102.210.247	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
146.185.250.2	147.237.72.217	Russian Federation	e.idf.il	ET SCAN NMAP -sS window 1024	1
103.240.113.113	147.237.76.30	Cambodia	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
98.119.105.221	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.77.234	Cote D'Ivoire	halag.idf.il	ET SCAN NMAP -sS window 4096	1
79.181.104.177	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
190.249.184.162	147.237.8.50	Colombia	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
175.204.97.12	147.237.0.35	Korea, Republic of	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
31.168.27.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.13.173	147.237.76.202	United Kingdom	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.18.126	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
121.201.27.61	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 2048	1
98.119.105.221	147.237.0.33	United States	idf.il	ET SCAN NMAP -f -sS	1
94.102.48.195	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.77.234	Cote D'Ivoire	halag.idf.il	ET SCAN NMAP -sS window 1024	1
190.249.184.162	147.237.8.50	Colombia	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
66.249.65.234	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	1
185.120.126.106	147.237.72.166		aka.idf.il	portscan: TCP Distributed Portscan	1
37.200.78.34	147.237.8.27	Russian Federation	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1

01-20-2016-20:04:01 to 01-20-2016-21:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.86.225	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
79.176.206.144	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
2.52.159.204	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.86.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
213.8.204.1	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.52.5.69	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
175.18.112.202	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
221.202.205.222	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
89.138.15.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
218.60.132.40	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
139.214.193.246	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
221.202.205.190	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
222.163.195.19	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
113.5.80.68	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
46.19.86.12	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.14	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
221.206.191.2	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
104.236.86.103		147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
46.19.86.130	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
218.60.123.59	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
222.163.195.35	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
46.19.85.223	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
94.230.86.186	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.159.204	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
222.163.195.35	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.66.184.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.104.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.145.58	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.66.187.118	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.121	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
149.78.245.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.127.152.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.5	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.173.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.0.110	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
218.60.123.59	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.46.39.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.46.39.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.223	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.52.5.69	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.5.69	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
5.102.254.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.32.179.85	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.8.204.1	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	169
37.142.64.129	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	85
213.8.204.1	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	66
149.78.244.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
104.236.86.103		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 104.236.86.103	Block	5
46.19.86.59	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	3
37.26.148.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.52.5.84	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.67.189.140	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	3
37.26.148.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.64.97.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.102.218.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
217.132.133.161	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
109.186.175.229	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	2
213.8.204.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.125.98.120	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
91.143.80.201	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
176.13.1.70	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
79.182.25.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
149.88.140.155	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9757-he/refuah.aspx	Block	1
198.20.69.77	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
2.54.135.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.82.77	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/popups/markivsachar.aspx	None	1
176.13.19.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.57.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.132.101.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
149.78.53.156	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
109.163.234.4	Romania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.176.126.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
185.3.147.216	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
2.52.159.204	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
66.249.78.51	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/1/106681.pdf	Block	1
46.19.85.204	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
149.88.217.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.61.129	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
217.132.133.161	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
79.179.118.87	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
109.253.211.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &SortDir in www.eitan.aka.idf.il/1103-he/eitan.aspx	None	1
198.58.102.155	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
2.54.161.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.64.97.217	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
86.97.30.82	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.116.245.177	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.3.147.216	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
82.80.198.164	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
41.102.196.77	Algeria	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
149.78.53.156	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1