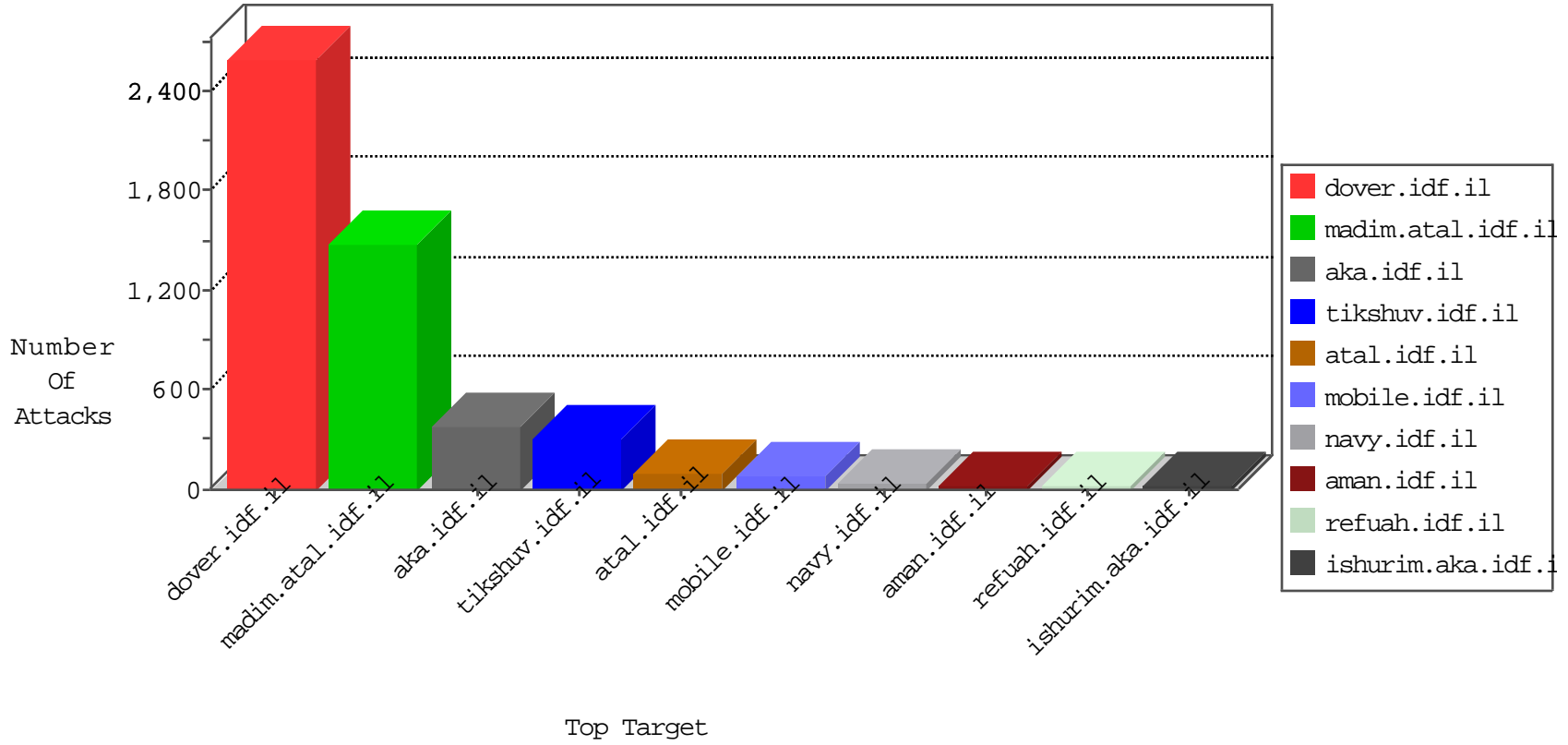


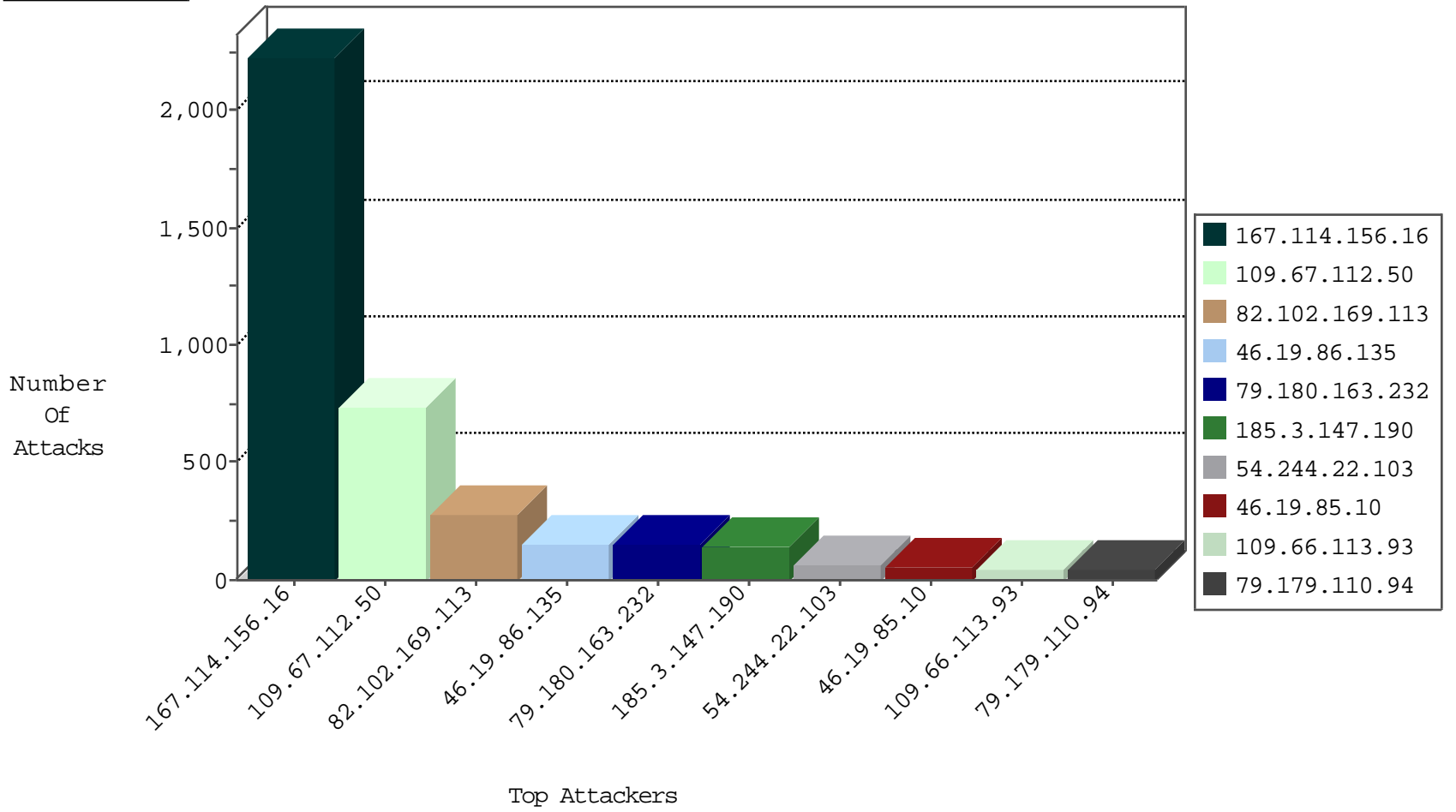
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	3028
66.102.9.21	United States	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
198.20.70.114	United States	147.237.76.198	e.ychalan.idf.il	Block_Udp_All_Nets	drop	1
77.125.132.249	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
5.189.146.119	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.37	China	147.237.76.198	e.ychalan.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.69.74	United States	147.237.76.196	e.sviva.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
79.177.131.241	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1
123.126.113.160	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.69.76	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
183.82.106.200	147.237.76.201	India	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
120.125.82.194	147.237.77.74	Taiwan	law.idf.il	ET SCAN NMAP -sS window 3072	1
120.125.82.194	147.237.77.74	Taiwan	law.idf.il	ET SCAN NMAP -f -sS	1
84.111.33.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.180.114.67	147.237.72.166	Poland	aka.idf.il	ET SCAN NMAP -sS window 2048	1
82.145.33.11	147.237.77.61	United Kingdom	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.76.196	United States	e.sviva.idf.il	ET DROP Dshield Block Listed Source	1
79.178.58.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.28.112.12	147.237.77.233	Moldova, Republic of	atal.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.234	147.237.76.147		chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
183.82.106.200	147.237.76.201	India	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
5.29.129.159	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
173.255.112.188	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
120.125.82.194	147.237.77.74	Taiwan	law.idf.il	ET SCAN NMAP -sS window 2048	1
109.253.141.22	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.180.114.67	147.237.72.166	Poland	aka.idf.il	ET SCAN NMAP -sS window 3072	1
84.109.136.59	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.180.114.67	147.237.72.166	Poland	aka.idf.il	ET SCAN NMAP -f -sS	1
80.230.69.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.165	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
185.130.5.234	147.237.76.196		e.sviva.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.87	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.234	147.237.8.14		e.orchot.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.179.55.205	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	33
5.22.135.93	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	30
46.19.85.207	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
77.125.132.249	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
46.19.85.81	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
46.19.85.123	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
37.26.149.229	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
2.54.146.159	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
80.215.160.137	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
31.168.137.30	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
212.76.127.44	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
46.121.123.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
79.177.150.152	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
31.168.137.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
68.180.229.94	United States	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	7
212.179.90.106	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
85.130.203.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.102.247.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.179.204.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.13.192.110	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.111.0.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.179.204.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.255	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.78.5	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.26.235	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.158.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.8.145	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.255	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.160.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.8.168	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.13.192.110	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.179.90.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.164.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.112.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	481
109.67.112.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	236
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	151
79.180.163.232	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	148
46.19.86.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	131
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	123
185.3.147.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
109.66.113.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
79.179.110.94	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	43
46.19.85.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
185.3.147.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	34
46.19.86.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
109.67.112.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	20
2.52.166.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
93.172.141.131	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
5.22.135.93	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
5.102.247.238	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 5.102.247.238	Block	5
84.229.152.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.2.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	3
176.13.3.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
50.243.254.210	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	3
109.253.147.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.3.147.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	3
50.243.254.210	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation lang in www.cogat.idf.il/1038-en/cogat.aspx	Block	3
109.253.207.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.64.13.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.57.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.178.11.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
50.243.254.210	United States	147.237.77.216	dover.idf.il	Parameter Type Violation tab in www.idf.il/1065-en/dover.aspx	Block	2
2.54.145.210	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
149.88.82.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.7.228	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.182.49.127	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
178.95.152.246	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/iturim/resources/images/body/images/main.jpg	Block	2
2.54.146.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
84.228.220.221	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/updateuserdetails.aspx	Block	2
37.238.112.18	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	2
46.19.85.148	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
77.126.22.24	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct142\$ct103\$ct103\$ddlQuestion in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
66.249.78.45	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
5.102.247.238	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz/resources/images/innerpage/goback.gif	Block	1
84.108.7.113	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/miyun/miyunselectquestionnaire.aspx	Block	1
212.143.38.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
50.243.254.210	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1065-en/dover.aspx	Block	1
109.64.11.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.0.238	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.182.236.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
194.150.168.95	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1