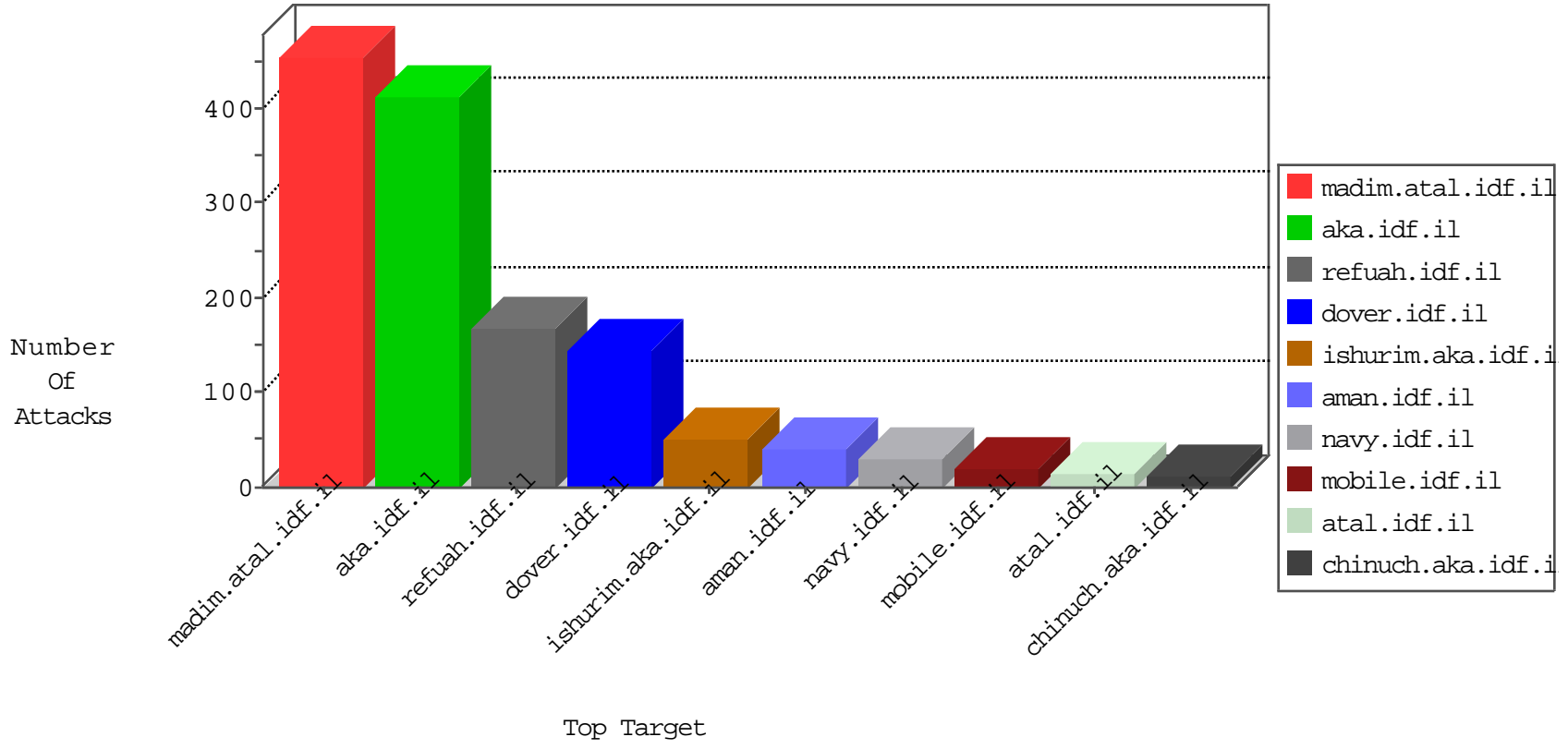


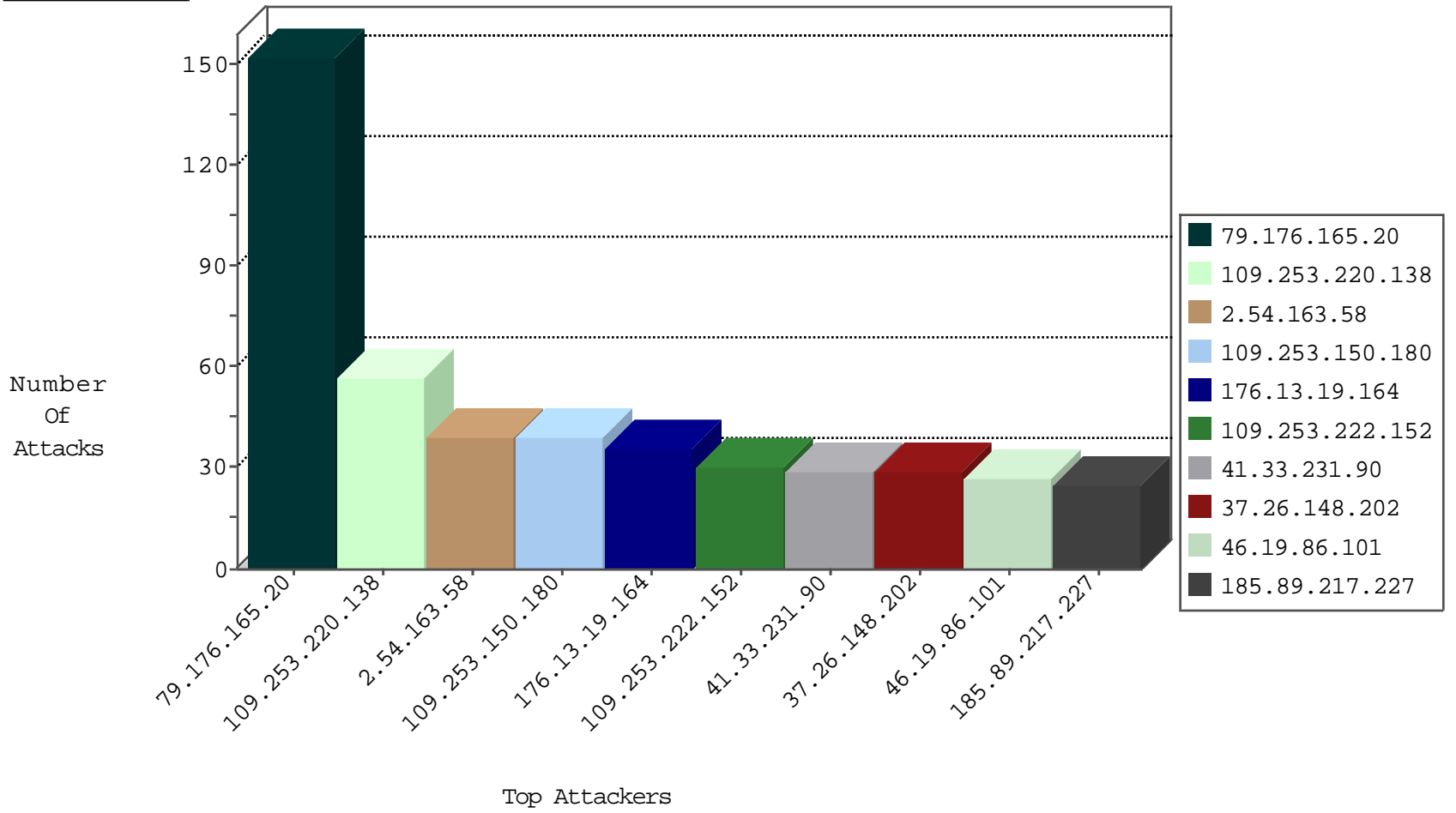
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
14.29.83.106	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
183.206.189.205	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
101.111.158.148	Japan	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
120.192.250.30	China	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
79.183.61.58	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1

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	2
79.177.170.93	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.91.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.28.215	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.130.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.29.203.226	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.158	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.179	147.237.76.34		yohalan.idf.il	ET SCAN Potential SSH Scan	1
2.54.139.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.11.17	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.223.238	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.56.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.30.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.0.34.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.75.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.145	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.172.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.9.42	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.14.239	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.136.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

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	29
46.19.86.101	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
185.89.217.227		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	21
46.19.86.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
62.0.200.125	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
185.89.217.226		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
109.253.212.53	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.60.117	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
185.89.217.234		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
62.0.207.1	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	11
185.89.217.231		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
185.89.217.235		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
80.179.91.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.89.217.229		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
185.89.217.224		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
188.120.148.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.233	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
185.89.217.233		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
80.246.136.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.26.148.194	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.121.122.98	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.180	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
185.89.217.228		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
80.254.150.79	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.94	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.0.200.125	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
188.120.148.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.179.115.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.89.217.230		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
2.52.170.98	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.13.22.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.143.163	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.64.158.221	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.210.187.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
217.194.207.24	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.54.34.124	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.52.143.163	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
80.246.138.183	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.72	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.130.132.157	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.118	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.89.217.232		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.165.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	92
79.176.165.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	60
109.253.150.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
2.54.163.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
109.253.220.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	37
176.13.19.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
109.253.222.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
37.26.148.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
176.13.17.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	23
109.253.220.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	20
176.13.9.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
109.253.220.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
80.179.115.9	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	7
176.13.16.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
212.143.38.222	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/4/110494.pdf	Block	4
109.253.129.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
2.54.183.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.145.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.128.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.145.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.136.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
85.250.188.68	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
46.19.85.115	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
185.89.217.229		147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2282.jpg	Block	1
66.249.78.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1397-he/atal.aspx	Block	1
217.194.207.24	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
108.59.8.68	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
58.8.148.60	Thailand	147.237.72.156	aman.idf.il	E-mail collector robots 14	Block	1
185.89.217.234		147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout.css	Block	1
37.60.40.220	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cpMain\$TochenPlaceHolder\$emailUpdate\$rpEmailSubjectsList\$ct101\$cbEmailSubject in www.aka.idf.il/main/gyus/faq.aspx	None	1
185.60.144.31	Switzerland	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/maslul.aspx?catid=61166	Block	1
80.179.115.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9235-he/refuah.aspx	Block	1
2.54.8.196	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
149.88.29.147	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;utm_campaign in www.aka.idf.il/	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
87.69.168.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.118	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
185.89.217.230		147.237.76.42	refuah.idf.il	URL is Above Root Directory www.refua.atal.idf.il/./images/shared/home.png	Block	1
79.178.174.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
8.37.70.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/dover.aspx&usg=alkjrhublknvnhx16aluup2ua4hhzsbda	Block	1
66.249.78.79	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 66.249.78.79	Block	1
217.194.207.24	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
58.8.148.60	Thailand	147.237.72.156	aman.idf.il	eMail Hoarding	Block	1
185.89.217.235		147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/2076.jpg	Block	1
109.65.31.71	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cpMain\$TochenPlaceHolder\$ct113\$ct102\$ct103\$txtField in aka.idf.il/main/gyus/questionnaire.aspx	None	1
37.142.68.8	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
185.89.217.224		147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/3435.jpg	Block	1