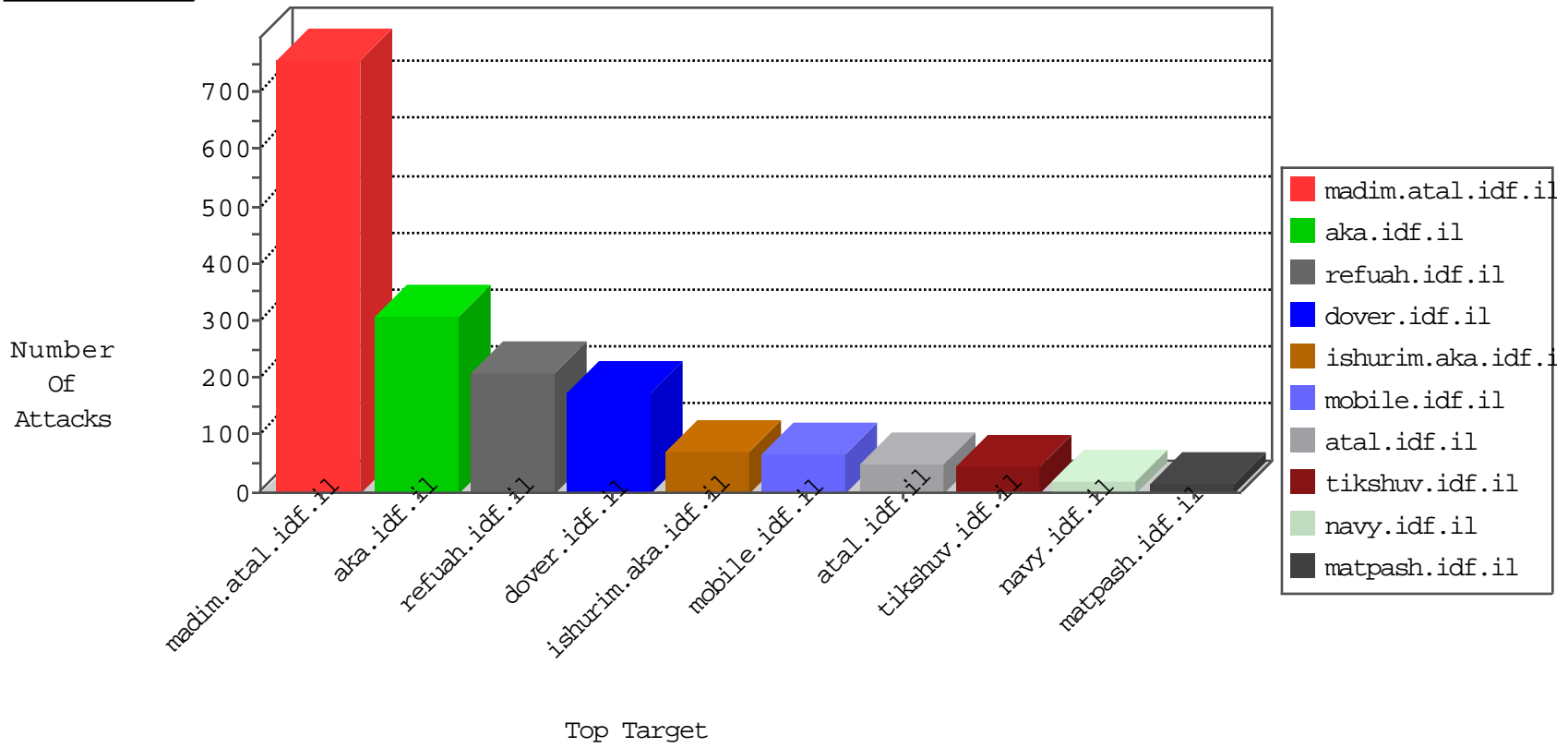


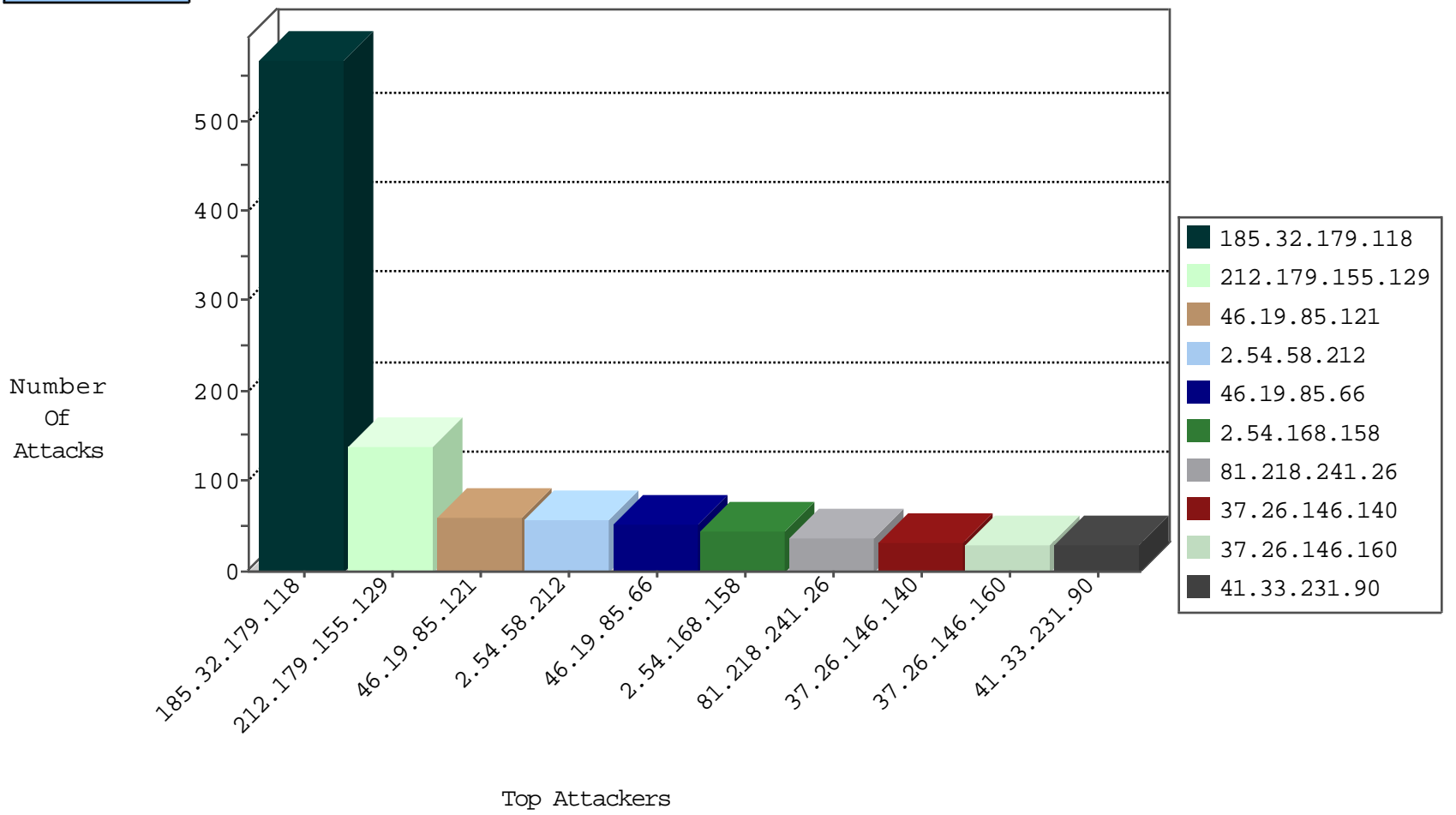
IDF Under Attack Daily Report



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	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	97
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
212.179.54.237	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
203.166.137.11	Singapore	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
74.122.110.53	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.36.124.17	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
203.166.137.12	Singapore	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
74.122.110.54	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.36.124.18	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
203.166.137.13	Singapore	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
187.160.156.170	Mexico	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
42.88.233.28	China	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
185.36.124.16	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
40.115.22.29	United States	147.237.0.19	madim.atal.idf.il	10711: HTTP: ZmEu Vulnerability Scanner	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
40.115.22.29	United States	147.237.0.15	kosher-kravi.idf.il	10711: HTTP: ZmEu Vulnerability Scanner	Block	1
40.115.22.29	United States	147.237.0.17	m.my-kosher-kravi.idf.il	10711: HTTP: ZmEu Vulnerability Scanner	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
218.246.0.97	147.237.76.148	China	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
134.191.232.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.48.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.216.191	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.77.76.3	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.21	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.88.192.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.113.125.11	147.237.77.170	Romania	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
80.179.31.248	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.11.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.81.175	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.155.129	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	127
46.19.85.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
37.26.146.160	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
2.52.7.24	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
37.26.146.140	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
194.90.225.101	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.128.8	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
2.52.7.24	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
31.210.186.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
138.134.192.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.29.168.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.26.146.140	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	8
192.118.12.102	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	8
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	7
217.21.11.152	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.54.171.180	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.29.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.198.15	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.71	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
94.188.248.70	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.187.99	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.66	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
94.188.248.70	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.23.207	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.78	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.44.160	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.146.140	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
185.5.220.163	Palestinian Territory, Occupied	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
81.4.217.86	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.179.155.129	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.179.155.129	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
182.232.40.27	Thailand	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.115.132.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
109.64.107.212	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
187.160.156.170	Mexico	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
2.52.45.182	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.160.242.40	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.160.242.40	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.89.217.228		147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.52.8.241	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.35	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.224.243.232	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
81.218.192.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	309
185.32.179.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	155
185.32.179.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
2.54.58.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
2.54.168.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
46.19.85.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
213.57.239.25	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 213.57.239.25	Block	17
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	12
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	8
46.19.85.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
87.69.62.227	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.62.227	Block	7
109.253.208.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.54.58.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
2.54.172.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.134.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.127.114.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.36.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
197.45.132.185	Egypt	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/xmlrpc.php	Block	3
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
197.45.132.185	Egypt	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	2
46.19.85.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.168.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.147.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.159.182	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
109.253.203.234	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
5.28.170.221	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceholder\$ct113\$ct101\$ct103\$cb1Question\$71 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
68.180.231.40	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/228-he/faq.aspx	Block	1
128.139.12.141	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/meitav	Block	1
212.179.155.129	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
109.65.181.175	Israel	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 2	Block	1
87.69.62.227	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	1
194.114.146.227	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
176.13.2.5	Israel	147.237.76.30	himush.idf.il	Distributed PHP Attempt	Block	1
109.65.181.175	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method \$ in URL x"b[[#26]]x'Èæ@Ã~Ãÿf=â,,çâ,,çÃ~Ã?ç[[#1]]x,Ã%Ã?^Ã?Ã±xçayÃ?Ö%Ã~Ö.Ãæx@æç;	Block	1
66.249.81.130	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
46.19.85.126	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
109.65.181.175	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name Ã%[[#3]]{ÃµyÃ?dÃ¶hÃ£[[#27]]Ã%[[#1]]S[[#12]]Ã°`Ã &Ã•Ã;Ã~ÃNÃªx*fÃ-Ãµ>GÃ"•Ãç[[#4]]Ã?Ã%Ã'Ãµ[[#7]]Ã<Ã°Ã<Ã<Ã%9Ã™[[#30]]Ã+ÃçÃ'Ã±TUÃ^	Block	1
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
141.212.122.112	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /x	Block	1
213.57.239.25	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
109.65.181.175	Israel	147.237.77.216	dover.idf.il	Malformed URL x"b[[#26]]x'Èæ@Ã~Ãÿf=â,,çâ,,çÃ~Ã?ç[[#1]]x,Ã%Ã?^Ã?Ã±xçayÃ?Ö%Ã~Ö.Ãæx@æç;	Block	1
89.138.121.247	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
37.26.146.160	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
176.13.2.5	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/xmlrpc.php	Block	1
80.246.133.242	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
2.54.128.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1