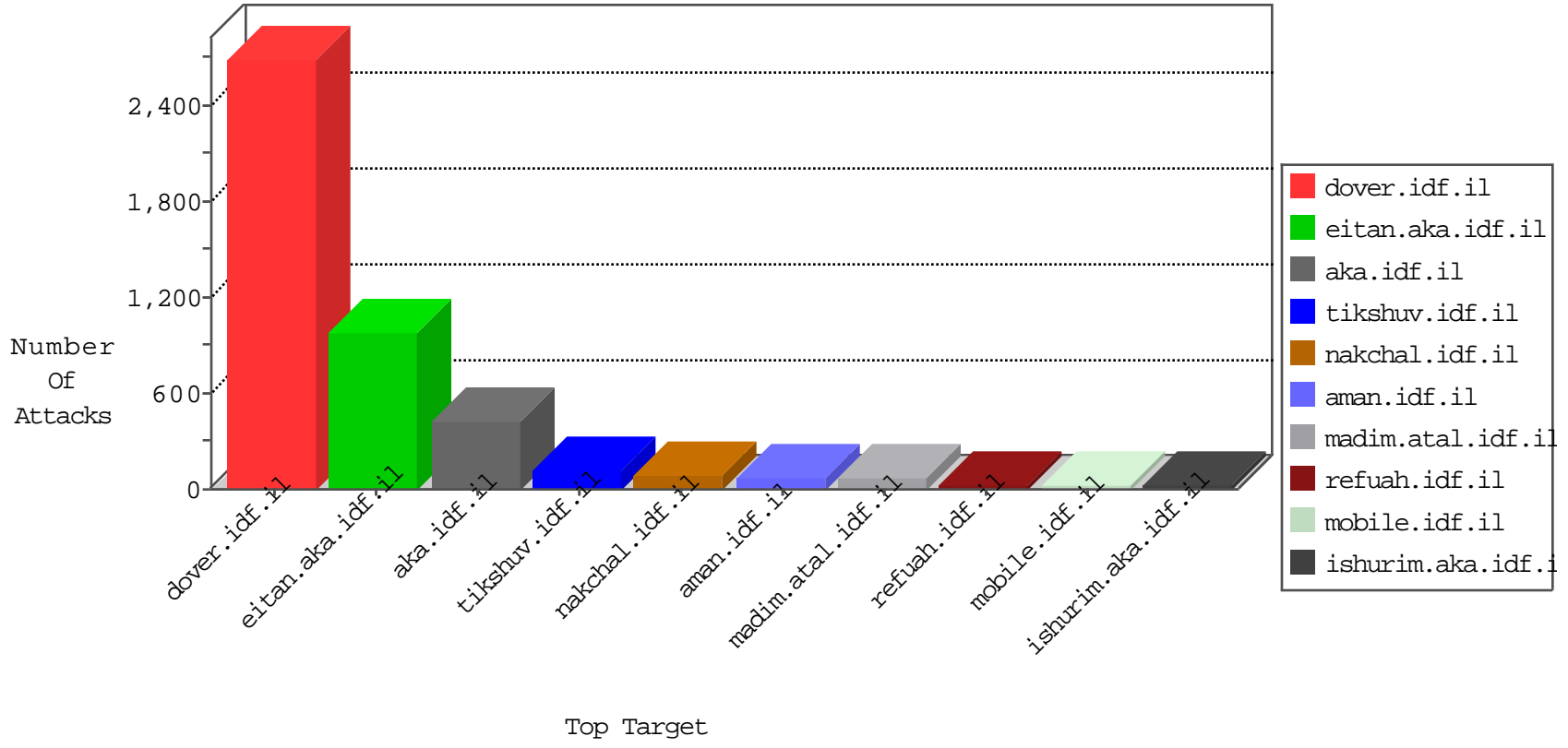


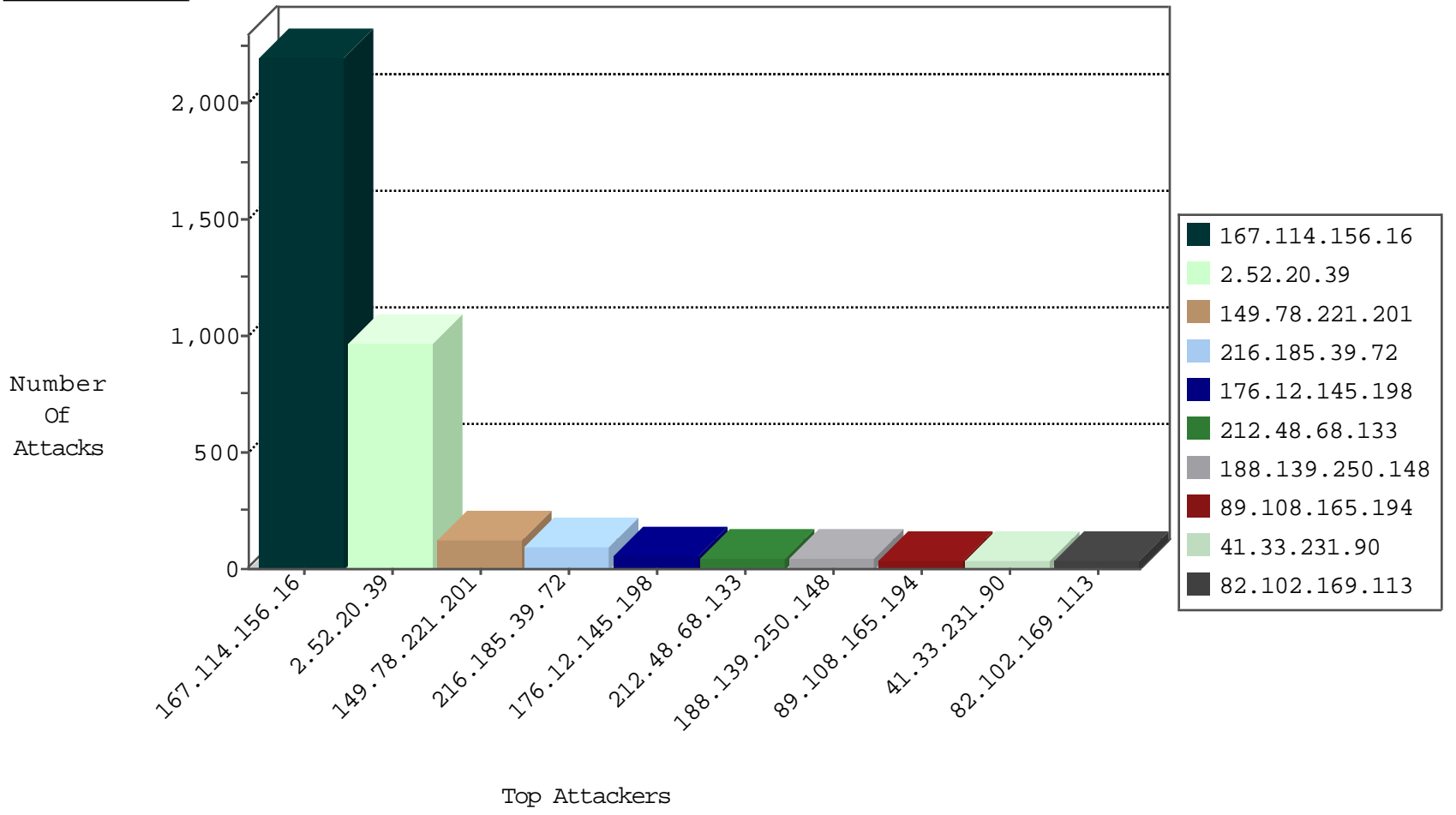
IDF Under Attack Daily Report



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	3169
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
216.185.39.72	United States	147.237.0.34	tikshuv.idf.il	Frk_Purple_Con_Limit_Http	drop	3
115.239.228.10	China	147.237.0.15	kosher-kravi.idf.il	Frk_Under_Attack_Con_Http	drop	2
216.185.39.72	United States	147.237.0.34	tikshuv.idf.il	Frk_Under_Attack_Con_Http	drop	2
207.104.161.245	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
115.239.228.10	China	147.237.0.15	kosher-kravi.idf.il	Frk_Purple_Con_Limit_Http	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.48.68.133	United Kingdom	147.237.0.34	tikshuv.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	15
212.48.68.133	United Kingdom	147.237.77.216	dover.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	10
212.48.68.133	United Kingdom	147.237.0.19	madim.atal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
212.48.68.133	United Kingdom	147.237.0.34	tikshuv.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	3
212.48.68.133	United Kingdom	147.237.77.216	dover.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	2
212.48.68.133	United Kingdom	147.237.0.19	madim.atal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.48.68.133	147.237.0.34	United Kingdom	tikshuv.idf.il	ET WEB_SERVER Muieblackcat scanner	3
115.84.83.157	147.237.77.216	Lao People's Democratic Republic	dover.idf.il	ET SCAN NMAP -sA (2)	2
212.48.68.133	147.237.77.216	United Kingdom	dover.idf.il	ET WEB_SERVER Muieblackcat scanner	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
94.102.60.89	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
213.57.161.42	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.94.21.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.102.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.80.155.223	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
70.165.1.67	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.77.243	United States	mobile.idf.il	ET DROP Dshield Block Listed Source	1
52.33.66.29	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.60.89	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
85.64.188.121	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.117.208.243	147.237.77.216		dover.idf.il	ET SCAN NMAP -sS window 1024	1
212.48.68.133	147.237.0.19	United Kingdom	madim.atal.idf.il	ET WEB_SERVER Muieblackcat scanner	1
79.180.200.210	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
207.7.112.132	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
68.204.111.212	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.26.146.234	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
146.185.250.2	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
109.186.191.172	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
2.52.20.39	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	828
149.78.221.201	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	77
216.185.39.72	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	71
149.78.221.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
89.108.165.194	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
93.173.248.222	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
188.139.250.148	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	20
188.139.250.148	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
213.57.130.104	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
8.37.226.238	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
2.52.22.217	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
216.185.39.72	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
213.57.135.216	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
213.57.135.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
188.120.148.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.52.48.248	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
94.230.86.204	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
213.57.130.155	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
192.115.177.202	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.52.28.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
85.64.159.155	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.134	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
84.111.184.160	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
82.102.169.113	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
81.218.3.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
80.246.136.106	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.206	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
62.90.165.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.28.147.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.142.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
197.33.72.42	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.228.249.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.129	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.254.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
82.102.169.113	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.48.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
213.57.130.155	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.47	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
5.22.129.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.178.184.213	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.146.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
149.88.54.29	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.48.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.20.39	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.20.39	Block	137
176.12.145.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
8.37.226.238	Anonymous Proxy	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
185.32.179.175	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	7
46.19.86.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.179.183.139	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	2
93.172.133.192	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
176.13.11.249	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
85.65.239.24	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
109.253.130.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.15.244	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
79.183.62.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.197	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
2.52.20.39	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	1
84.109.240.171	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
46.19.86.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.4.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
46.19.85.213	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
149.78.93.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
36.229.182.50	Taiwan	147.237.77.216	dover.idf.il	Directory Traversal (In URL)	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/gyus/general.aspx	Block	1
212.143.85.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
54.153.33.233	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
192.114.91.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.52.175.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.6.147	Israel	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
46.19.86.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.74.121	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.238	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.126.225.171	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.15	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.231.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.28.164.118	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
84.111.232.137	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.120.190.210	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
176.13.4.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.213	Israel	147.237.77.216	dover.idf.il	Malformed URL __atuvs=5676deb3c95e6eab000	Block	1
149.78.221.201	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakchal.aspx	Block	1
79.180.5.239	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.235.103.203	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/1/size338x0/1671.jpg	Block	1
36.229.182.50	Taiwan	147.237.77.216	dover.idf.il	Directory Traversal - 16	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/gyus/forum/asp/showforum.asp	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/gyus/gyus/general.aspx	Block	1