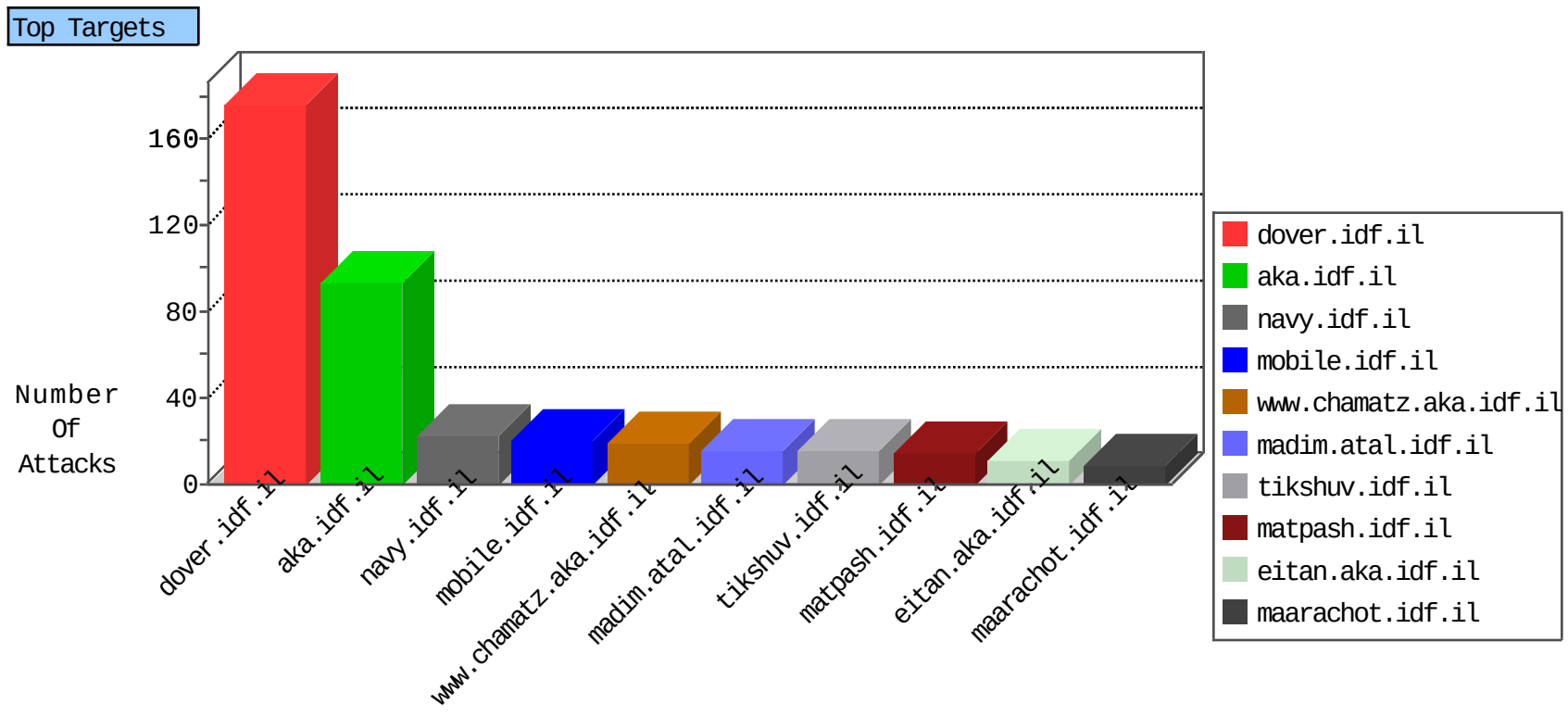
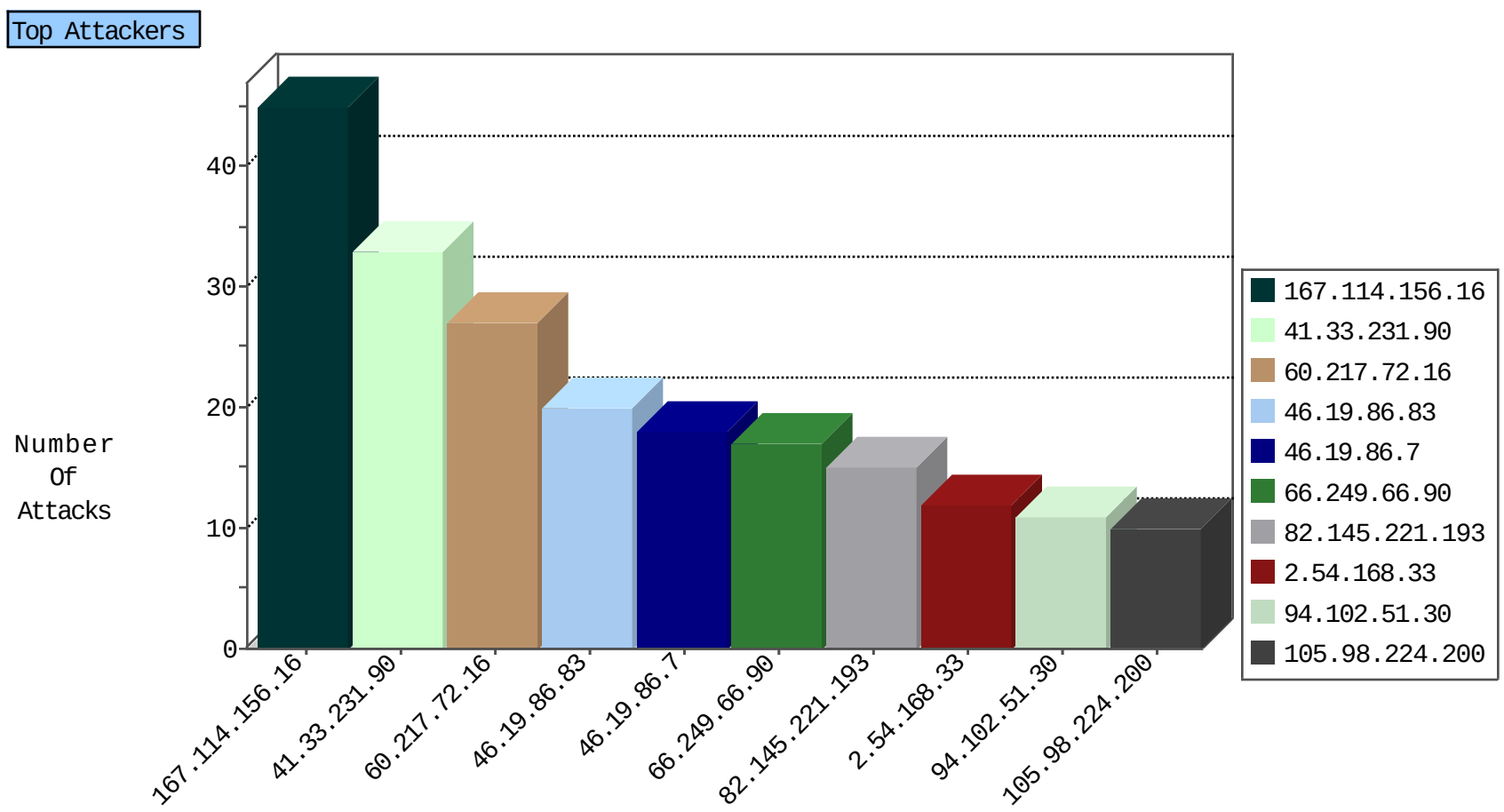
01-09-2016-09:04:04 to 01-09-2016-10:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-09-2016-09:04:04 to 01-09-2016-10:04:04

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	1101
27.152.75.144	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	2
59.45.240.39	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
208.67.1.60	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
60.217.72.16	China	147.237.76.197	e.himush.idf.il	JLM_Purple_Con_Limit_Https	drop	1
146.185.239.100	Russian Federation	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
208.67.1.60	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
60.217.72.16	China	147.237.76.202	e.halag.idf.il	JLM_Purple_Con_Limit_Https	drop	1
208.67.1.60	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
115.239.228.10	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Http	drop	1
60.217.72.16	China	147.237.76.196	e.sviva.idf.il	JLM_Purple_Con_Limit_Https	drop	1
123.179.228.60	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

01-09-2016-09:04:04 to 01-09-2016-10:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
104.45.132.180	United States	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
198.20.69.78	United States	147.237.8.24	e.lifestyle.idf.i	13840: TLS: OpenSSL Heartbeat Packet	Block	1
198.20.69.78	United States	147.237.76.197	e.himush.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

01-09-2016-09:04:04 to 01-09-2016-10:04:04

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
60.217.72.16	147.237.76.39	China	mobile.meitav.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
60.217.72.16	147.237.77.216	China	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
199.191.56.188	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
60.217.72.16	147.237.76.31	China	nakchal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
193.104.41.54	147.237.76.201	Moldova, Republic of	e.atal.idf.il	ET SCAN Potential SSH Scan	1
60.217.72.16	147.237.0.19	China	madim.atal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
193.104.41.54	147.237.76.196	Moldova, Republic of	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
60.217.72.16	147.237.0.16	China	my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.221.22	147.237.77.216	China	dover.idf.il	SQL generic sql with comments injection attempt - GET parameter	1
58.253.96.122	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
180.97.221.22	147.237.77.216	China	dover.idf.il	SQL 1 = 1 - possible sql injection attempt	1
58.253.96.122	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1
180.97.221.22	147.237.77.216	China	dover.idf.il	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access	1
94.102.48.195	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
60.217.72.16	147.237.76.42	China	refuah.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
199.191.56.188	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
60.217.72.16	147.237.76.38	China	e.e.meitav.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
193.104.41.54	147.237.76.202	Moldova, Republic of	e.halag.idf.il	ET SCAN Potential SSH Scan	1
60.217.72.16	147.237.76.30	China	himush.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
193.104.41.54	147.237.76.199	Moldova, Republic of	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
60.217.72.16	147.237.0.17	China	m.my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
193.104.41.54	147.237.0.35	Moldova, Republic of	akaws.idf.il	ET SCAN Potential SSH Scan	1
60.217.72.16	147.237.0.15	China	kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.221.22	147.237.77.216	China	dover.idf.il	SQL Injection - Select From	1
58.253.96.122	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
180.97.221.22	147.237.77.216	China	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	1
5.102.253.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.97.221.22	147.237.77.216	China	dover.idf.il	ET WEB_SERVER MYSQL SELECT CONCAT SQL Injection Attempt	1

01-09-2016-09:04:04 to 01-09-2016-10:04:04

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	31
46.19.86.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
82.145.221.193	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
2.54.168.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.7	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
79.181.102.213	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
31.13.165.25	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.28.166.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.86.7	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.117.39.243	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
65.55.210.138	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.120.126.49		147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.187	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.228.111.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
85.65.71.200	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.147.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
73.151.107.100	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.179.23.127	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.62.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.15.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.110.11	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
87.69.0.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
37.142.243.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.117.69.189	Israel	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
85.65.71.200	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.102.253.9	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.175.13.138	Germany	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
87.69.0.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.3.147.221	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.64	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
81.169.237.146	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
105.98.224.200	Algeria	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
218.6.155.58	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
27.55.47.63	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
94.102.51.30	Netherlands	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	1
149.88.247.166	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
83.244.54.90	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
106.75.199.201	China	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
74.82.47.19	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
94.102.51.30	Netherlands	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1

01-09-2016-09:04:04 to 01-09-2016-10:04:04

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
5.22.131.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	3
84.228.62.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.128.45	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
85.65.96.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.249	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
46.120.230.39	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.120.230.39	None	2
5.29.92.129	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	2
176.13.12.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	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
85.65.230.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.34.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
105.98.224.200	Algeria	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /robots.txt	Block	1
60.217.72.16	China	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.94.189.213	Israel	147.237.0.34	tikshuv.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 84.94.189.213	Block	1
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	1
180.97.221.22	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/news/html/	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13115-en/dover	Block	1
60.217.72.16	China	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 60.217.72.16 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
93.172.163.81	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 93.172.163.81 (Open Mode)	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/2616.jpg	Block	1
173.252.88.182	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
105.98.224.200	Algeria	147.237.77.235	sviva.idf.il	Unauthorized URL Access to /robots.txt	Block	1
60.217.72.16	China	147.237.76.30	himush.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.108.11.238	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
40.77.167.21	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list20050529.htm	Block	1
185.120.126.49		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/giyus/general.aspx	None	1
60.217.72.16	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
109.64.2.5	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
60.217.72.16	China	147.237.0.15	kosher-kravi.idf.il	Multiple Untraceable SSL Sessions from 60.217.72.16 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
93.172.163.81	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
74.82.47.4	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
5.29.205.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/2423.jpg	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
60.217.72.16	China	147.237.76.31	nakchal.idf.il	Multiple Untraceable SSL Sessions from 60.217.72.16 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
40.77.167.23	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/8/4148.pdf&gt	Block	1
216.218.206.68	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
60.217.72.16	China	147.237.0.16	my-kosher-kravi.idf.il	Multiple Untraceable SSL Sessions from 60.217.72.16 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
105.98.224.200	Algeria	147.237.77.74	law.idf.il	Unauthorized URL Access to /robots.txt	Block	1
79.182.31.249	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
17.138.54.87	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	1