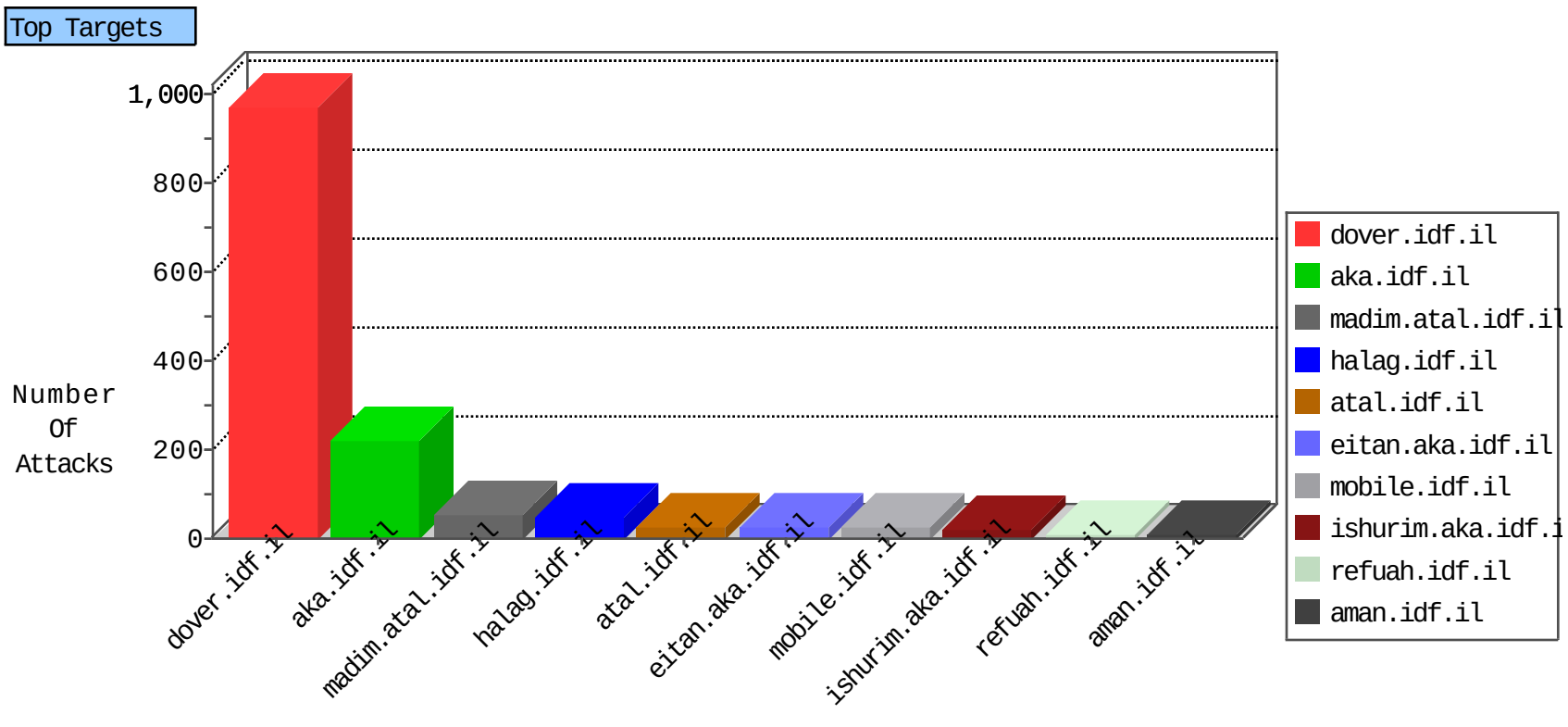
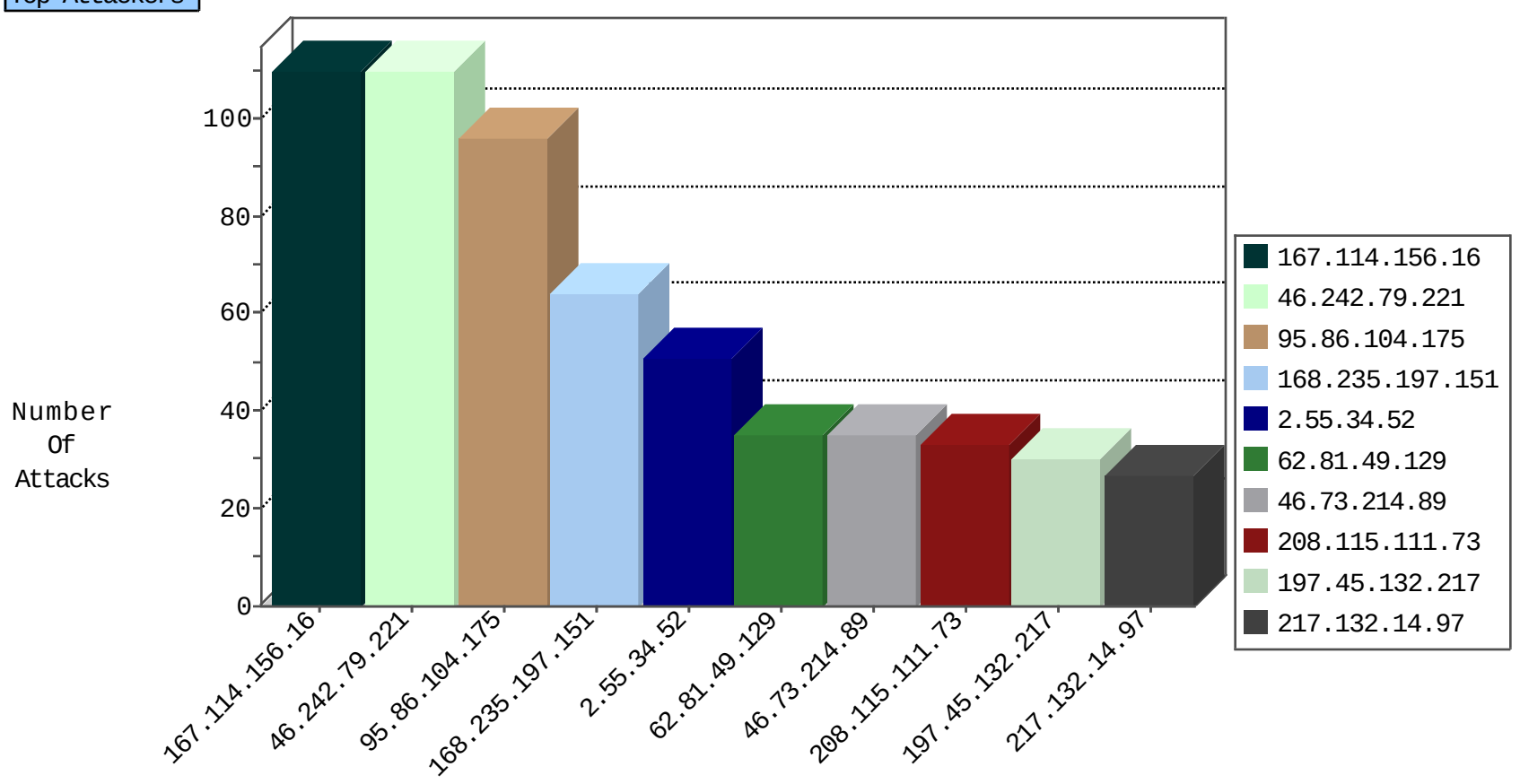
04-26-2016-20:04:08 to 04-26-2016-21:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-26-2016-20:04:08 to 04-26-2016-21:04:08

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	HTTP-POST-Segmented-DoS	dest-reset	4965
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3795
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2581
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	10
109.64.90.154	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
5.164.83.208	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
168.235.197.151	United States	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
95.213.255.38	Russian Federation	147.237.76.200	eitan.aka.idf.i	Block_Udp_All_Nets	drop	1

04-26-2016-20:04:08 to 04-26-2016-21:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-26-2016-20:04:08 to 04-26-2016-21:04:08

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
176.13.2.67	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.81.230	147.237.77.176	Europe	matpash.idf.il	ET SCAN NMAP -sA (2)	2
98.119.105.221	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
82.117.208.243	147.237.0.200		m4u.idf.il	ET SCAN NMAP -sS window 1024	1
208.115.111.73	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
195.216.176.244	147.237.8.46	Latvia	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
98.119.105.221	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -f -sS	1
80.82.78.38	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
23.96.109.87	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 4096	1
198.20.69.98	147.237.76.200	United States	eitan.aka.idf.il	ET DROP Dshield Block Listed Source	1
195.216.176.244	147.237.8.28	Latvia	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1

04-26-2016-20:04:08 to 04-26-2016-21:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.242.79.221	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	110
95.86.104.175	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	88
168.235.197.151	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
46.73.214.89	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
62.81.49.129	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
217.132.14.97	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
149.62.12.246	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
5.164.83.208	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
107.167.113.148	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
95.221.238.34	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
75.119.230.50	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
186.67.116.154	Chile	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
198.58.102.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
5.63.250.18	Hungary	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
40.77.167.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
207.46.13.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
84.94.169.114	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
70.29.103.44	Canada	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
207.46.13.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.9.212	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
157.55.39.147	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
31.168.169.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
198.251.60.85	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
95.86.104.175	Israel	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
88.243.160.173	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.64.90.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.0	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.224.140	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.30.236.89	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
172.56.30.245	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.2.67	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.146.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.116.204.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.3.144.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.0	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.14.128	Israel	147.237.77.243	mobile.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
2.55.34.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
2.53.48.44	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.20.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.139.10.158	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.177.26.166	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/registrationwizard/register.aspx	Block	1
131.253.25.191	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.111.242.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.147	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
199.30.24.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.26.149.234	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
109.3.144.122	France	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.177.26.166	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatesMonth in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
157.55.39.147	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.102.146.88	Switzerland	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/tmp/php.class.php	Block	1
84.200.45.38	Germany	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
199.30.24.163	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.46.42.14	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
109.65.121.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.94.169.114	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
164.132.161.33	Italy	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL /english/organization/homefront/homefront2.stm#012	Block	1
5.102.147.191	Switzerland	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/tmp/php.class.php	Block	1
85.65.132.162	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.177.16.48	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.177.16.48	Block	1
40.77.167.57	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
199.30.25.30	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.65.224.140	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.108.18.212	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
176.13.14.128	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
23.81.70.146	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
85.65.132.162	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.177.26.166	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
51.255.65.11	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/62532.pdfg2=whvq9jgvov3igm-oflegda	Block	1
217.132.14.97	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.253.225.118	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.109.241.153	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/2423.jpg	Block	1
23.81.70.148	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/shared/usercontrols/headerupper/	Block	1

04-26-2016-20:04:08 to 04-26-2016-21:04:08