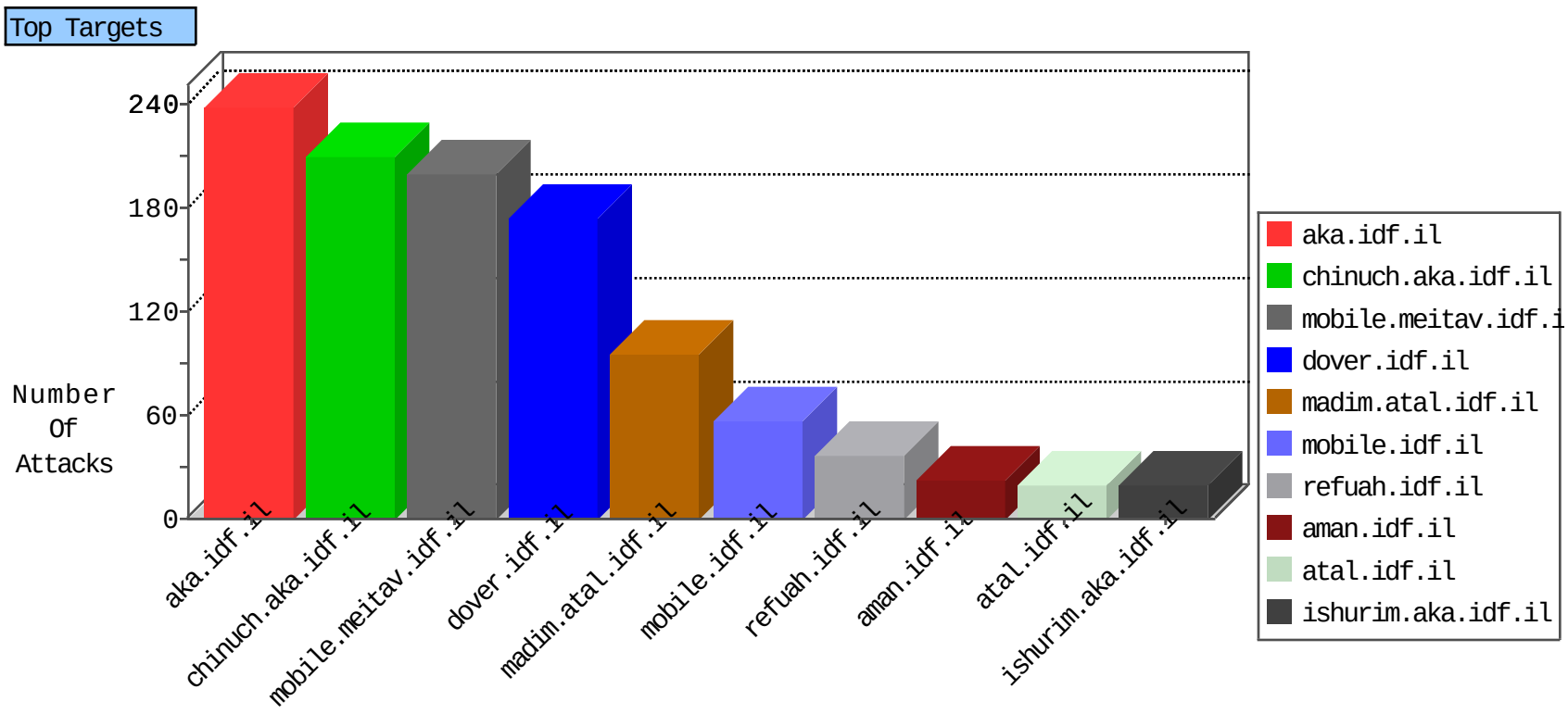
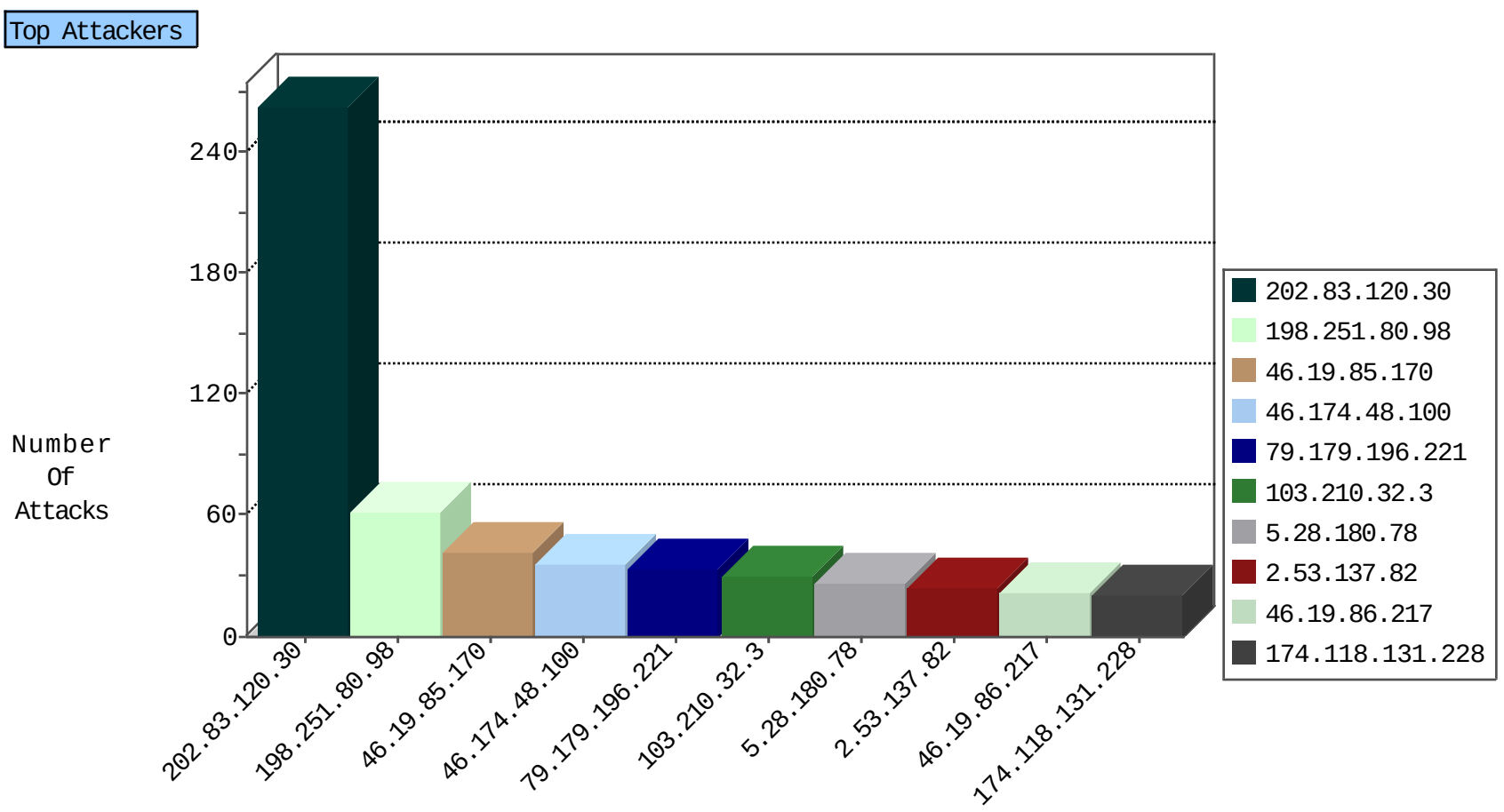
09-25-2016-21:04:02 to 09-25-2016-22:04:02

IDF Under Attack
Daily Report





09-25-2016-21:04:02 to 09-25-2016-22:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.239	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	44
109.67.49.97	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
93.174.93.218	Netherlands	147.237.76.86	navy.idf.il	block-sp-traf1	forward	1
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	1
123.151.42.61	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
66.240.219.146	United States	147.237.76.30	himush.idf.il	Black List	drop	1

09-25-2016-21:04:02 to 09-25-2016-22:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.254.143.238	France	147.237.77.216	dover.idf.i	C1000074: HTTP: majestic bot	Permit	17
89.44.144.244	Romania	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
212.68.146.35	Israel	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
151.80.31.163	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
88.231.132.131	Turkey	147.237.72.166	aka.idf.il	C1000016: HTTP: administrator in URI	Permit	1
88.231.132.131	Turkey	147.237.72.166	aka.idf.il	C1000018: HTTP: access to administrator/index.php -> Quarantine	Permit	1

09-25-2016-21:04:02 to 09-25-2016-22:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
89.44.144.244	147.237.77.74	Romania	law.idf.il	SQL Injection - Select From	7
212.68.146.35	147.237.77.233	Israel	atal.idf.il	SQL Injection - Select From	5
84.52.124.134	147.237.76.147	Russian Federation	chinuch.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.162.154.120	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
218.205.151.198	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 2048	1
66.249.64.160	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
211.149.244.79	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
178.213.24.212	147.237.77.74	Russian Federation	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
116.108.33.164	147.237.76.44	Vietnam	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
106.120.209.153	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -f -sS	1
82.162.154.120	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
80.246.139.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.205.151.198	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -f -sS	1
211.149.244.79	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
183.35.51.200	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
146.200.148.0	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	1
106.120.209.153	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 2048	1
92.42.162.161	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN NMAP -sS window 1024	1

09-25-2016-21:04:02 to 09-25-2016-22:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	Invalid ACK number	monitor	35
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	34
46.19.85.170	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	33
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	30
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	29
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
174.118.131.228	Canada	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
5.28.180.78	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	14
5.28.180.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	13
2.54.96.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.53.148.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
103.210.32.3		147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
2.53.137.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
105.107.146.68	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
2.55.128.110	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
103.210.32.3		147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
198.251.80.98	United States	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
103.210.32.3		147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
176.13.237.72	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
77.139.209.169	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
198.251.80.98	United States	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	8
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	8
79.181.184.168	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
174.118.131.228	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
176.13.225.160	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.137.82	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
198.251.80.98	United States	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	6
37.26.149.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		alert	6
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
2.53.137.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
2.53.15.138	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.199.57.207	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.209.167	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.217	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.177.240.209	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.137	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.137.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.217	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.137	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.202.255	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
176.13.11.192	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5

09-25-2016-21:04:02 to 09-25-2016-22:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.196.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
46.19.85.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
93.174.93.218	Netherlands	147.237.76.86	navy.idf.il	Multiple NULL Character in Method from 93.174.93.218	Block	3
213.57.201.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.0.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.179.186.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.67.227.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.148.169	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.42	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
88.231.132.131	Turkey	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
66.249.79.41	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding jzj9c^XCz2B_1;Q2&-N@ ob-P/tUX]lbvhezwj_IWc in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
185.29.11.14	Latvia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
37.26.147.251	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
84.109.68.48	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
77.139.66.245	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
66.249.64.145	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/mobile/	Block	1
172.56.36.23	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1
2.53.15.138	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	1
88.231.132.131	Turkey	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
77.124.16.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.174.93.218	Netherlands	147.237.76.86	navy.idf.il	NULL Character in Method	Block	1
37.142.223.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.111.240.230	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 84.111.240.230	Block	1
77.139.69.145	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/brothers/kurs/default.asp	Block	1
66.249.66.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2422.jpg	Block	1
2.53.37.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
88.231.132.131	Turkey	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/admin.php	Block	1
80.246.137.102	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
217.169.179.10	Czech Republic	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.62.231	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	1
84.229.70.76	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
79.76.0.101	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash/sheelon.aspx	Block	1
66.249.75.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
176.13.225.160	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
89.138.110.8	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
81.218.8.170	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
77.138.133.62	France	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
123.125.71.31	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
62.219.161.62	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
87.70.19.159	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.76.83	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2277.jpg	Block	1
176.13.226.44	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
93.174.93.218	Netherlands	147.237.76.86	navy.idf.il	Multiple Illegal Byte Code Character in Method from 93.174.93.218	Block	1
5.102.242.118	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.94.184.21	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
77.138.243.23	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1

09-25-2016-21:04:02 to 09-25-2016-22:04:02