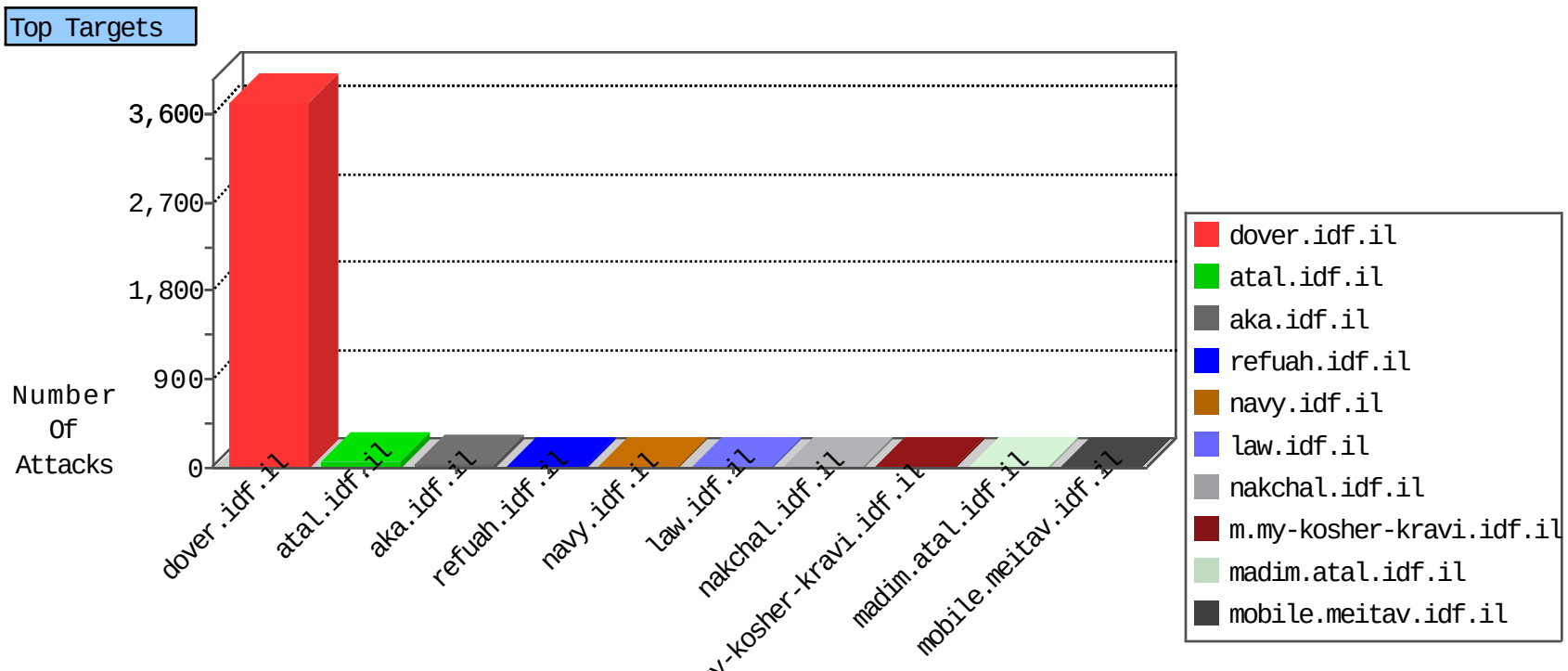
11-07-2015-07:04:02 to 11-07-2015-08:04:02

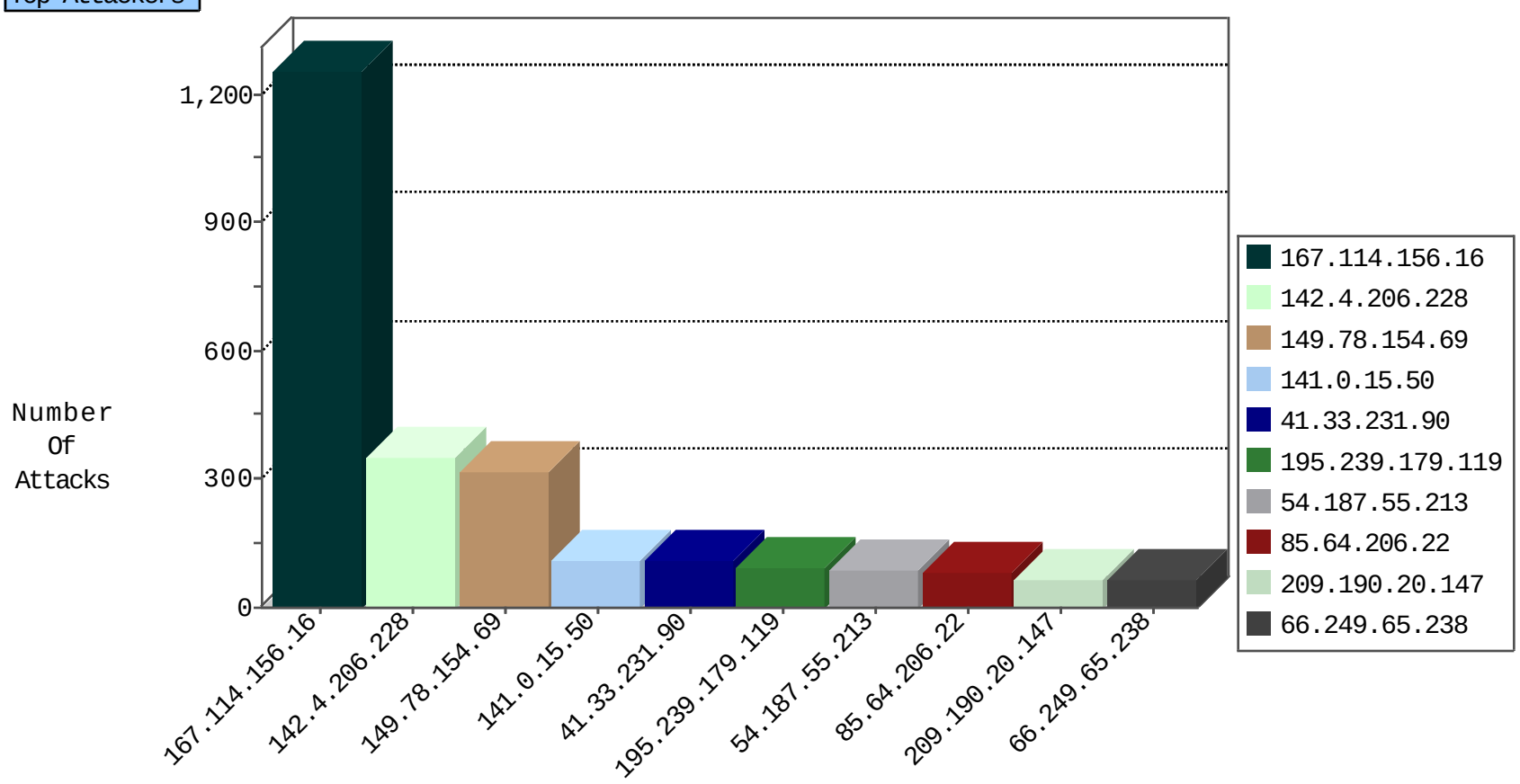
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-07-2015-07:04:02 to 11-07-2015-08:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3190
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2508
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	732
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	452
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	295
109.66.190.39	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
185.26.182.37	Europe	147.237.77.233	atal.idf.il	Frk_Purple_Con_Limit_Http	drop	3
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
185.26.182.37	Europe	147.237.77.233	atal.idf.il	Frk_Under_Attack_Con_Http	drop	1
190.200.147.103	Venezuela	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1
204.42.253.132	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

11-07-2015-07:04:02 to 11-07-2015-08:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
209.190.20.147	United States	147.237.76.31	nakchal.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1

11-07-2015-07:04:02 to 11-07-2015-08:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
142.4.206.228	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP WEB-INF access	20
209.190.20.147	147.237.77.216	United States	dover.idf.il	SQL 1 = 1 - possible sql injection attempt	16
142.4.206.228	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	6
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.75.206	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.7	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.224	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
66.249.65.238	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
193.105.134.220	147.237.0.16	Sweden	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.37	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
188.138.9.51	147.237.8.46	Germany	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.37	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential SSH Scan	1
59.2.190.99	147.237.8.45	Korea, Republic of	e.eitan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.82.64.37	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN Potential SSH Scan	1
31.6.71.154	147.237.76.39	Poland	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.37	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
80.82.64.37	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
80.82.64.37	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -sS window 1024	1
193.107.17.72	147.237.0.17	Seychelles	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.37	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
190.73.174.236	147.237.8.46	Venezuela	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
78.142.19.47	147.237.76.196	Bulgaria	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.37	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1
80.82.64.37	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
80.82.64.37	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
31.6.71.154	147.237.76.30	Poland	himush.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.37	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
210.61.150.154	147.237.0.19	Taiwan	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
80.82.64.37	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1
80.82.64.37	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1

11-07-2015-07:04:02 to 11-07-2015-08:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
142.4.206.228	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	321
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	310
141.0.15.50	Europe	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	108
195.239.179.119	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	91
54.187.55.213	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	84
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	81
85.64.206.22	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	74
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	64
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	50
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	50
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	50
85.64.162.187	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	49
69.157.160.82	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	46
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	45
66.249.65.238	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
185.26.182.37	Europe	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	42
94.43.135.245	Georgia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
66.249.65.231	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
209.190.20.147	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
66.249.65.224	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
66.249.88.81	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
31.210.176.181	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
40.77.167.39	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
207.46.13.11	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
82.80.25.221	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
198.58.102.155	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
157.55.39.89	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
79.177.102.115	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
66.249.65.224	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
198.58.102.49	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
139.162.216.112	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
50.116.30.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
79.181.5.146	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
162.243.199.26	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
198.58.99.82	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
157.55.39.31	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
65.19.138.34	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
109.66.190.39	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
91.228.167.130	Slovakia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	11
66.249.65.238	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
185.26.182.37	Europe	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
40.77.167.59	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
66.249.65.231	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
46.19.85.35	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
157.55.39.180	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9

11-07-2015-07:04:02 to 11-07-2015-08:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
209.190.20.147	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 209.190.20.147	Block	14
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	5
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	4
208.115.111.72	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.111.72	Block	3
79.182.14.210	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 79.182.14.210	None	3
109.67.168.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
142.4.206.228	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1115-ar/dover.aspx	Block	2
209.190.20.147	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1111-he/nakhal.aspx	Block	2
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.65.237	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/library/manage/resource/getfilecontent.hh.asp	Block	1
66.249.67.147	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/	Block	1
185.25.151.159	Poland	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	1
62.210.88.201	France	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to www.google.pl/search	Block	1
66.249.93.132	Israel	147.237.76.42	refuah.idf.il	URL is Above Root Directory www.refua.atal.idf.il/../../images/shared/menustrech.png	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.51	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1111-he/nakhal.aspx	Block	1
209.190.20.147	United States	147.237.77.216	dover.idf.il	Parameter Type Violation nid in www.idf.il/atal1/izkor/nofel_main.asp	Block	1
66.249.67.224	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 66.249.67.224 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
185.49.14.190	Poland	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/2254.jpg	Block	1
109.67.105.132	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
67.55.84.212	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
209.190.20.147	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 209.190.20.147	Block	1
157.55.39.63	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
209.190.20.147	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
66.249.67.224	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/2370.jpg	Block	1
185.49.14.190	Poland	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
185.25.151.159	Poland	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	1
76.218.104.163	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/2414.jpg	Block	1
185.49.14.190	Poland	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on testp2.czar.bielawa.pl/testproxy.php	Block	1
142.4.206.228	United States	147.237.77.216	dover.idf.il	Multiple Directory Traversal - 3(+) from 142.4.206.228	Block	1
68.180.228.175	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/228-he/faq.aspx	Block	1
209.190.20.147	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucFaqControl$txtSearch in nakhal.idf.il/1085-he/nakhal.aspx	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
185.25.151.159	Poland	147.237.76.42	refuah.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
5.254.97.85	Romania	147.237.77.74	law.idf.il	Parameter Type Violation PageNum in www.law.idf.il/327-he/patzar.aspx	Block	1
79.182.14.210	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding NunE4%;TmMjN	None	1

11-07-2015-07:04:02 to 11-07-2015-08:04:02