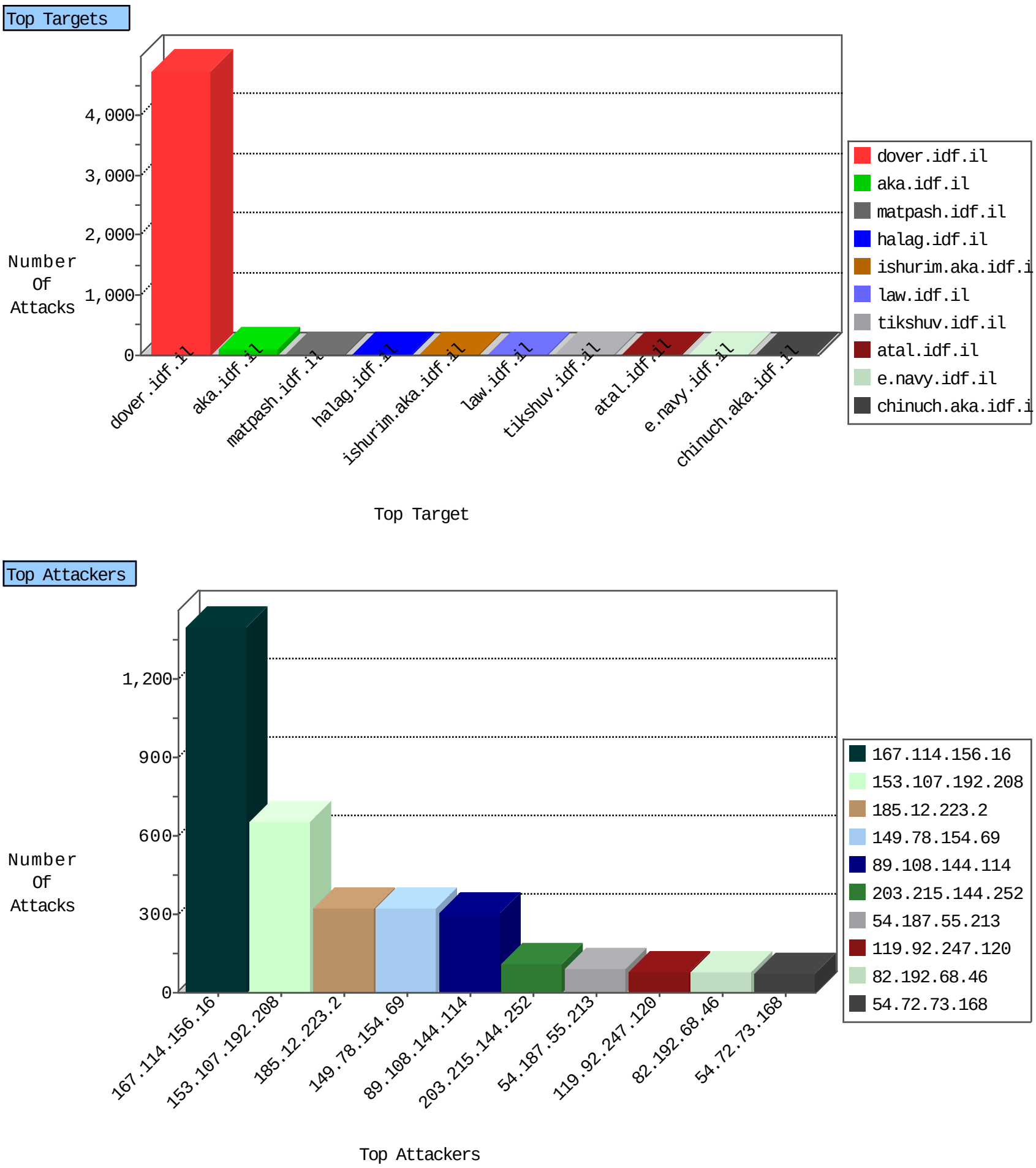
11-06-2015-03:04:00 to 11-06-2015-04:04:00

IDF Under Attack Daily Report



11-06-2015-03:04:00 to 11-06-2015-04:04:00

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	2487
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	439
2.54.176.30	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2
66.240.236.119	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
10.0.0.2		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
180.97.106.36	China	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
180.97.106.161	China	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	drop	1
66.240.236.119	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
94.102.52.213	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

11-06-2015-03:04:00 to 11-06-2015-04:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
202.124.109.87	New Zealand	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	20

11-06-2015-03:04:00 to 11-06-2015-04:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.124.109.87	147.237.72.166	New Zealand	aka.idf.il	SQL Injection - Select From	22
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	8
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
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in URI	3
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Cookie	2
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	SERVER-WEBAPP TRACE attempt	2
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	Admin login page scan - Havij	2
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	SERVER-WEBAPP adminlogin access	2
61.64.14.170	147.237.8.27	Taiwan	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
49.74.112.87	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt	1
198.52.97.84	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	SQL Injection - Select From	1
188.138.9.51	147.237.77.179	Germany	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
185.81.158.163	147.237.77.121		e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	SERVER-IIS cmd.exe access	1
119.90.138.60	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	1
112.216.8.157	147.237.72.167	Korea, Republic of	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt	1
112.216.8.157	147.237.72.167	Korea, Republic of	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	1
82.117.208.243	147.237.8.45		e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
54.72.73.168	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt	1
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	1
185.81.158.163	147.237.77.121		e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
1.161.246.20	147.237.0.34	Taiwan	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	1
120.107.144.49	147.237.77.170	Taiwan	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	1
119.42.127.232	147.237.8.28	Thailand	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	GPL WEB_SERVER /etc/passwd	1
112.216.8.157	147.237.72.167	Korea, Republic of	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	1
89.248.174.106	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1

11-06-2015-03:04:00 to 11-06-2015-04:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
153.107.192.208	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	656
185.12.223.2	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	324
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	320
89.108.144.114	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	302
203.215.144.252	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	110
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	90
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
119.92.247.120	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
2.54.45.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
216.4.56.146	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
99.238.52.167	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
201.52.36.247	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
5.102.254.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.249.69.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
157.55.39.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
188.29.164.28	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
66.249.88.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.88.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
79.176.150.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
66.249.69.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.88.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
41.234.50.29	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
5.29.80.92	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
198.58.102.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.69.34	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.69.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
157.55.39.208	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
157.55.39.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
70.138.169.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
31.210.186.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.181.171.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
109.66.41.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
129.81.167.124	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	9
99.110.72.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9

11-06-2015-03:04:00 to 11-06-2015-04:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/navy/html/toolfs.asp	Block	2
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/navy/html/toolfs.asp	Block	2
66.249.67.204	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
31.193.51.17	France	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
66.249.69.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19336-he/dover.aspx	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.120	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
84.111.14.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
37.142.68.63	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
157.55.39.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/navy/html/toolfs.asp	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/smalim/showbig.aspx	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
109.65.105.123	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
62.210.88.201	France	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.google.pl/search	Block	1
173.252.90.120	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/1/size220x0/1751.jpg	Block	1
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
114.97.53.176	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.65.86	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
178.255.87.242	United Kingdom	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/robots.txt	Block	1
69.171.230.118	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on 147.237.0.34/sip_storage/files/1/size220x0/1751.jpg	Block	1
66.249.67.196	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
31.13.102.123	Ireland	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on 147.237.0.34/901-7935-he/tikshuv.aspx	Block	1
149.78.213.206	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/901-7935-he/tikshuv.aspx	Block	1
66.249.69.38	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1772	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/haredim/general.aspx	None	1
203.215.144.252	Australia	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx	Block	1
79.197.203.120	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1

11-06-2015-03:04:00 to 11-06-2015-04:04:00