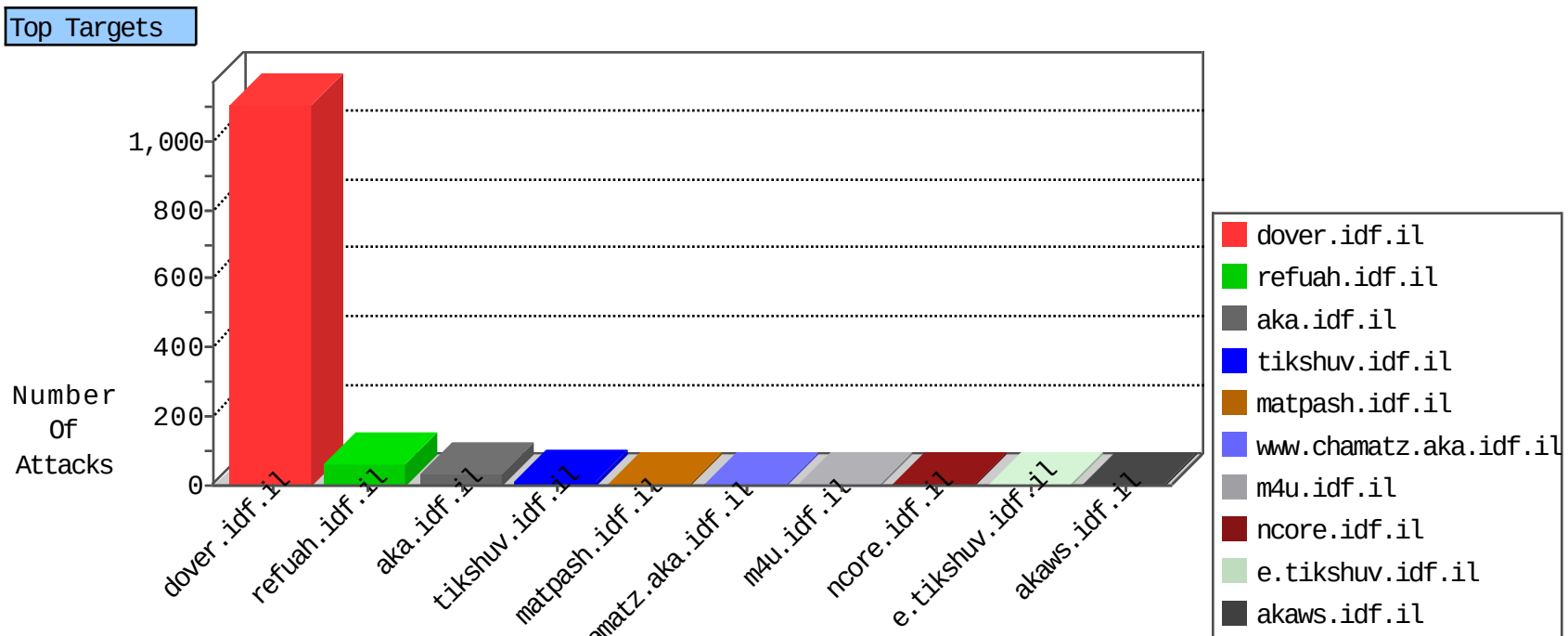
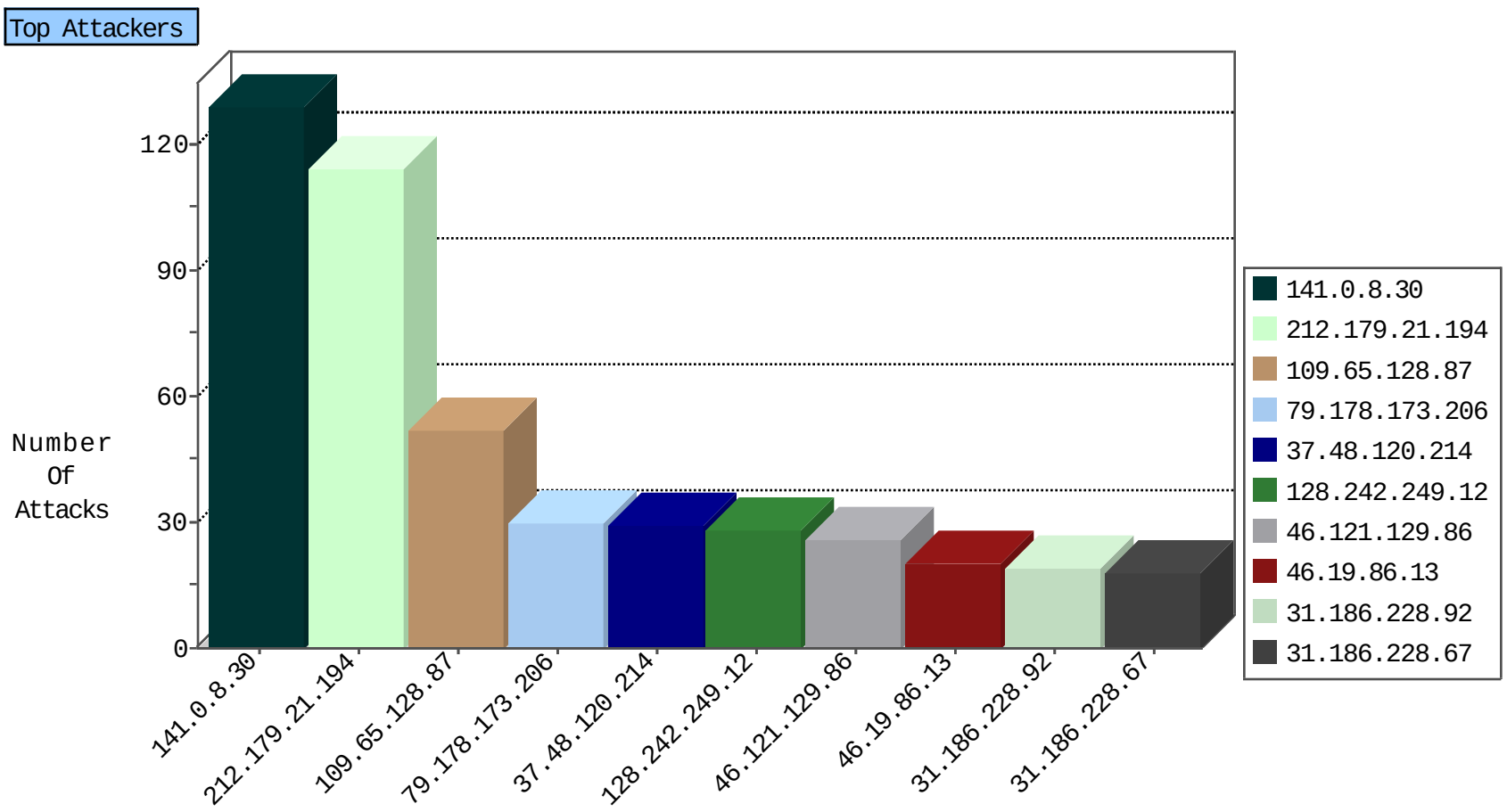
05-09-2015-08:03:00 to 05-09-2015-09:03:00

IDF Under Attack
05-09-2015-08:03:00

Top Targets



Top Attackers



05-09-2015-08:03:00 to 05-09-2015-09:03:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
222.66.55.240	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2

05-09-2015-08:03:00 to 05-09-2015-09:03:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	28
71.6.167.142	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1

05-09-2015-08:03:00 to 05-09-2015-09:03:00

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
192.151.147.94	United States	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
192.151.147.94	United States	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
79.180.148.67	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.255.85.228	Netherlands	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
188.138.9.51	Germany	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
183.136.216.4	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
221.226.106.188	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.4	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
221.226.106.188	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
121.88.5.177	Korea, Republic of	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
210.61.150.154	Taiwan	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 2048	1
94.131.14.10	Russian Federation	147.237.77.74	law.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
199.101.186.200	United States	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.67	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
198.20.69.74	United States	147.237.77.216	dover.idf.il	ET DROP Dshield Block Listed Source	1
61.160.224.128	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
192.151.147.94	United States	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
5.255.85.228	Netherlands	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
183.136.216.4	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
221.226.106.188	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.4	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
221.226.106.188	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
121.88.5.177	Korea, Republic of	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
210.61.150.154	Taiwan	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 4096	1
104.192.0.20		147.237.77.178	e.matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
210.61.150.154	Taiwan	147.237.77.216	dover.idf.il	ET SCAN NMAP -f -sS	1
199.101.186.200	United States	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.67	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5800-5820	1

05-09-2015-08:03:00 to 05-09-2015-09:03:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
141.0.8.30	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	129
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	114
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
109.65.128.87	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	26
46.121.129.86	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
109.65.128.87	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	alert	25
46.19.86.13	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
31.186.228.29	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
31.186.228.67	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
31.186.228.92	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
31.186.228.28	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
31.186.228.31	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
87.69.20.224	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
31.186.228.87	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
31.186.228.24	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
31.186.228.89	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
31.186.228.62	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
31.186.228.30	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
64.46.23.242	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
31.186.228.23	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
31.186.228.93	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
31.186.228.63	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
31.186.228.65	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
31.186.228.25	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
31.186.228.64	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
31.186.228.68	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
31.186.228.60	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
31.186.228.95	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
31.186.228.96	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
31.186.228.90	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
31.186.228.26	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
157.55.39.162	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
31.186.228.61	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
216.223.27.53	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
31.186.228.170	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
31.186.228.58	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
31.186.228.91	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
79.179.60.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
79.180.18.135	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
79.180.148.67	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
31.186.228.88	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
31.186.228.32	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
79.181.151.214	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.64.168	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6

05-09-2015-08:03:00 to 05-09-2015-09:03:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	3
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
162.243.81.121	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 162.243.81.121	Block	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	2
61.135.190.68	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
184.105.247.195	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.223	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/mobile/	Block	1
31.193.51.59	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
61.135.190.70	China	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on 147.237.0.19//	Block	1
198.20.69.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
66.249.78.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/	Block	1
37.115.187.54	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
79.176.184.71	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
61.135.190.72	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
199.47.81.11	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1568-	Block	1
157.55.39.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/1213.stm	Block	1
66.249.78.80	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
37.150.162.209	Kazakstan	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
175.44.16.10	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
109.65.128.87	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.99	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/about/pages/aboutus.aspx	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	1
66.249.78.160	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/portalmi	Block	1
54.147.176.220	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
180.76.5.67	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
142.54.161.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17055-en/dover.aspx/trackback/	Block	1
66.249.64.245	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18590-he/dover.aspx	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/mce_src=	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1

05-09-2015-08:03:00 to 05-09-2015-09:03:00