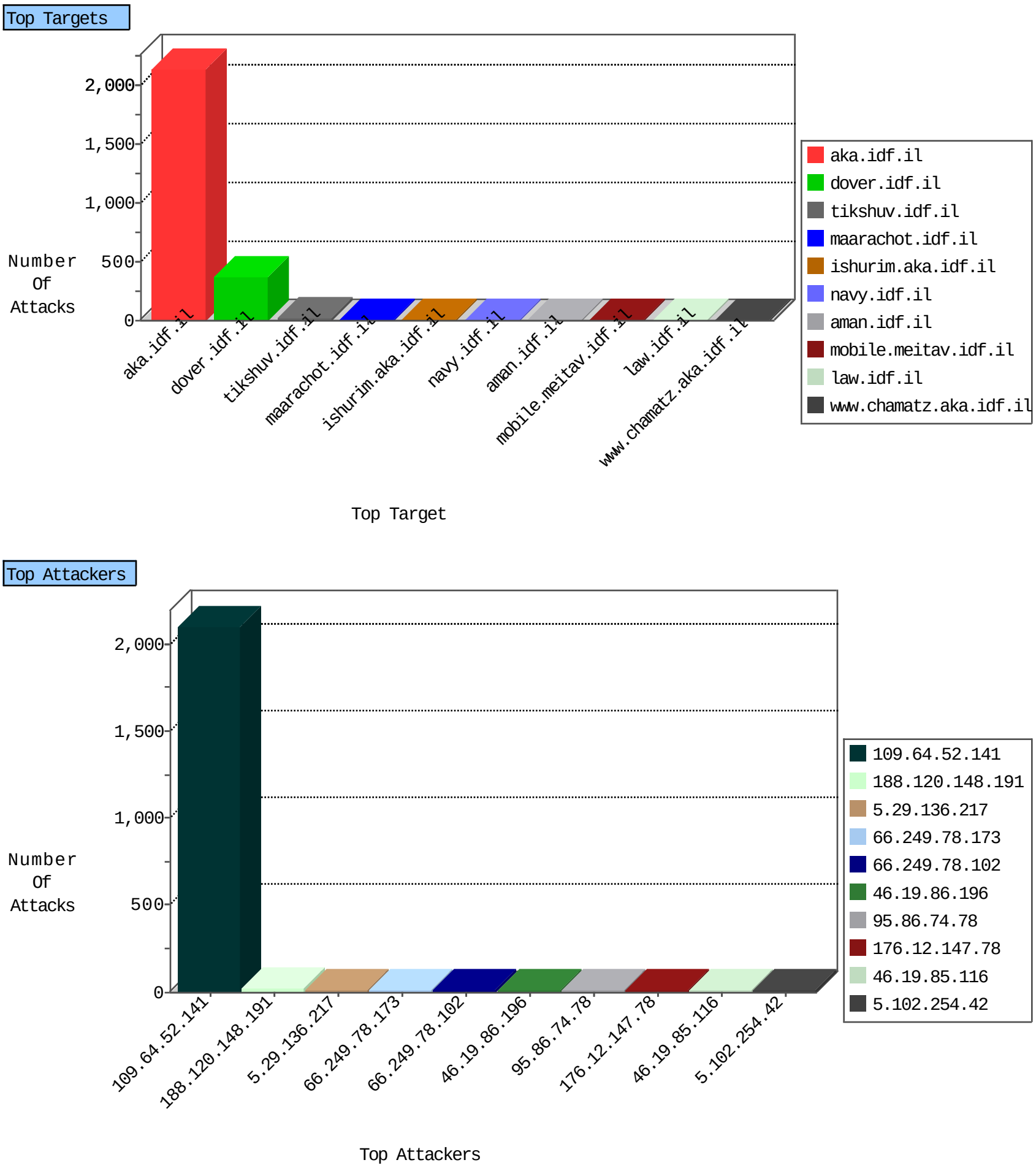
04-28-2015-01:03:08 to 04-28-2015-02:03:08

IDF Under Attack
04-28-2015-01:03:08



04-28-2015-01:03:08 to 04-28-2015-02:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.94	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	365
85.65.225.21	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
95.86.74.78	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
198.12.64.170	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
198.12.64.170	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
66.240.192.138	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

04-28-2015-01:03:08 to 04-28-2015-02:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.64.52.141	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	2104
66.240.236.119	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	2
198.20.69.98	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	2
66.240.236.119	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	2
71.6.135.131	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.86	navy.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
85.250.86.244	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
87.68.211.94	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.37	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1

04-28-2015-01:03:08 to 04-28-2015-02:03:08

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
66.249.67.30	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
81.145.191.82	United Kingdom	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
81.145.191.82	United Kingdom	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
213.210.205.2	Saudi Arabia	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
199.116.250.199	United States	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.132.118	Russian Federation	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
91.217.90.49	Ukraine	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
81.145.191.82	United Kingdom	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
66.249.69.122	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
50.7.217.50	Czech Republic	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
213.210.205.2	Saudi Arabia	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
202.71.25.29	India	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
91.238.134.92	Poland	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
91.217.90.49	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1

04-28-2015-01:03:08 to 04-28-2015-02:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
188.120.148.191	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
5.29.136.217	Israel	147.237.0.34	tikshuv.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	14
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
176.12.147.78	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
46.19.85.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
89.149.110.134	Moldova, Republic of	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
81.218.66.107	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.78.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
176.12.143.195	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.86.196	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
176.12.149.89	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
5.102.254.42	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
46.19.86.196	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	6
176.12.149.167	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
176.12.139.150	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.86.210	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
66.249.78.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
66.249.78.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
79.181.99.58	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
95.86.74.78	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
95.86.74.78	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
5.102.254.42	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
46.19.86.148	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
88.80.131.240	Bulgaria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
176.12.149.192	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
176.12.149.192	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
190.148.148.221	Guatemala	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	4
96.224.5.142	United States	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	4
176.12.137.229	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
124.13.188.142	Malaysia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.176	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
109.253.144.15	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
109.64.143.176	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	3
105.156.255.211	Morocco	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
73.181.149.9	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
190.237.115.145	Peru	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
108.53.59.131	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.116.211.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.64.143.176	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
84.228.79.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
149.78.99.152	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.117.194.57	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
104.32.108.33		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
87.68.156.45	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
46.119.113.155	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	3
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	2
66.249.64.73	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//m/	Block	1
185.32.178.221	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
142.54.161.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1559-en/dover.aspx/trackback/	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
80.246.130.109	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/6/×©×§×•×¤×™™×ª 3	Block	1
66.249.64.24	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//templates/sendtofriend/sendtofriend.aspx	Block	1
157.55.39.208	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
96.224.5.142	United States	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
68.180.228.34	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.64.75	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/m/	Block	1
188.165.15.13	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21744-ar/idfgdover.aspx	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/home.asp/info.asp	Block	1
46.19.86.98	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
84.108.109.182	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan/main/m...91&docid=63754	Block	1
66.249.78.51	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/mobile/	Block	1
66.249.64.27	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//	Block	1
157.55.39.210	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/	Block	1
109.253.130.216	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
192.157.245.129	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/pricing	Block	1
66.249.64.77	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//m/	Block	1
157.55.39.15	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/maatzar.stm	Block	1
46.101.178.175	Russian Federation	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//templates/sendtofriend/sendtofriend.aspx	Block	1
66.249.64.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1086-7837-he/dover.aspx	Block	1
185.5.249.191		147.237.72.166	aka.idf.il	CVE-2013-4810: JBoss Remote Command Execution 1	Block	1
109.253.146.137	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.187.110.98	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to testp1.piwo.pila.pl/testproxy.php	Block	1
66.249.67.30	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/templatecontrols/links/undefined	Block	1
157.55.39.24	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-14816-he/dov	Block	1
87.68.211.94	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1097-he/dover.aspx	Block	1
66.249.64.66	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
185.5.249.191		147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/invoker/ejbinvokerservlet/	Block	1
134.249.53.8	Ukraine	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
5.29.136.217	Israel	147.237.0.34	tikshuv.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 5.29.136.217	Block	1
79.177.174.47	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
192.187.110.98	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	1
66.249.69.122	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	1
66.249.64.4	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
95.90.241.158	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/desault.aspx	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.109	Block	1

04-28-2015-01:03:08 to 04-28-2015-02:03:08