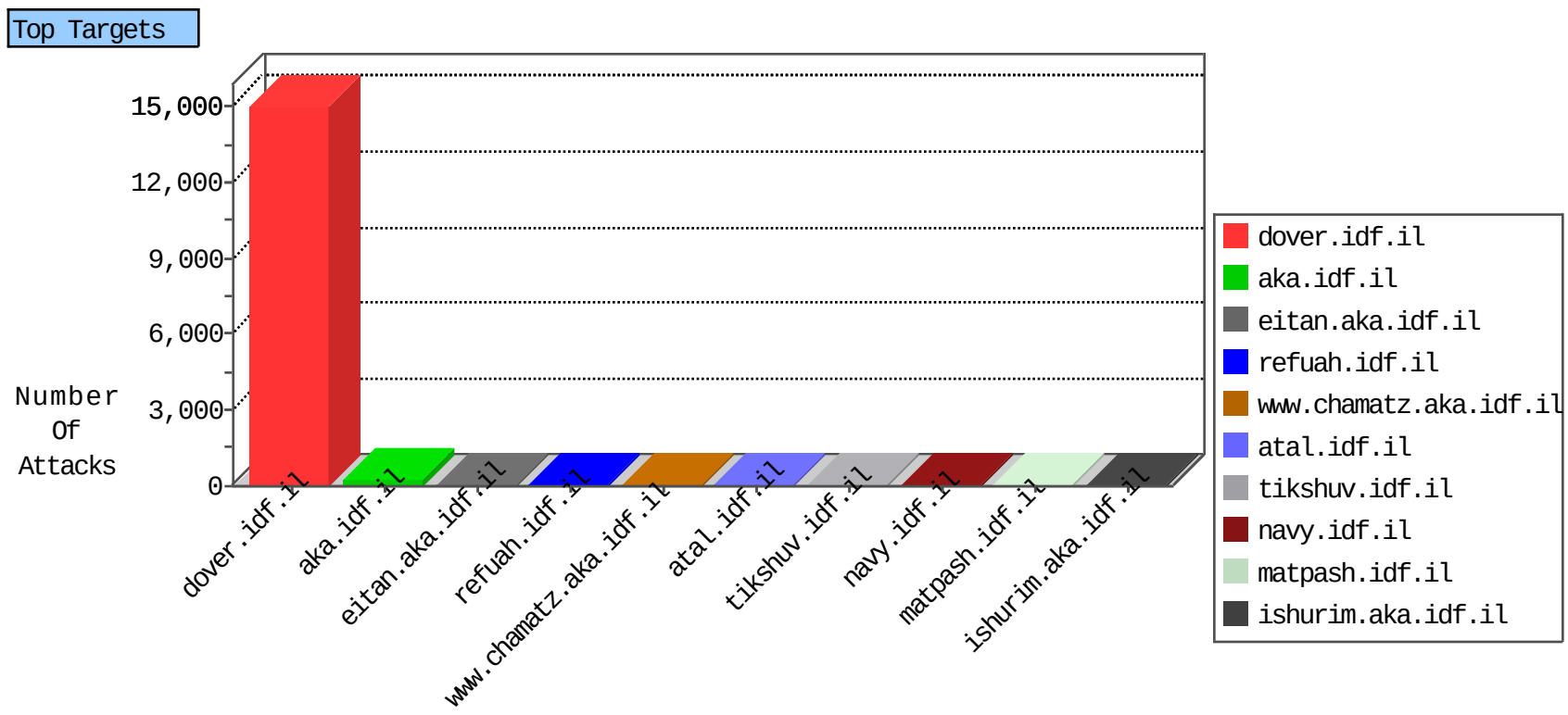
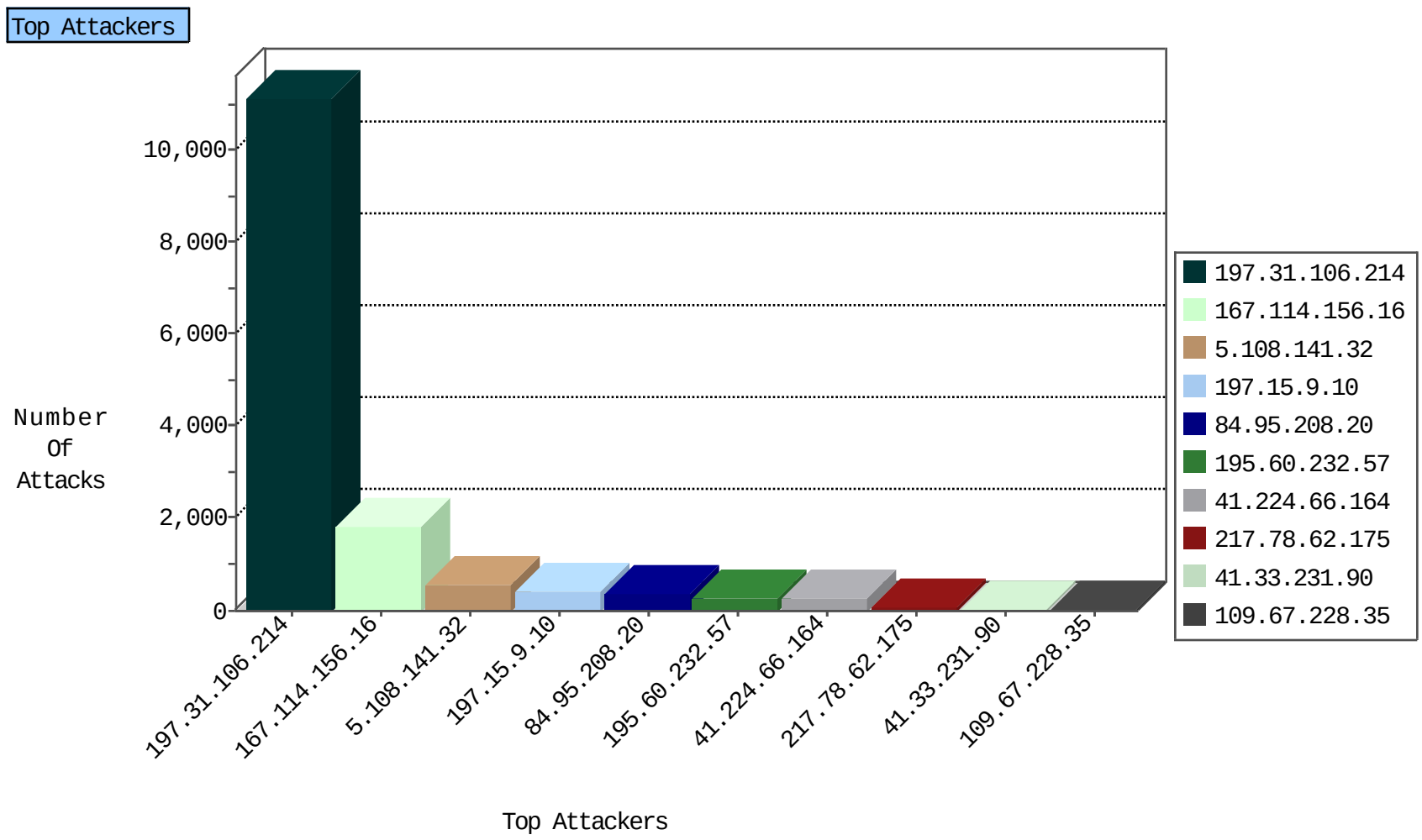
04-10-2016-02:04:08 to 04-10-2016-03:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-10-2016-02:04:08 to 04-10-2016-03:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3197
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1842
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	938
197.15.9.10	Tunisia	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-product3	dest-reset	376
41.224.66.164	Tunisia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	285
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	58
197.15.9.10	Tunisia	147.237.77.216	dover.idf.il	Web-etc/passwd-Dir-Traversal	dest-reset	8
197.15.9.10	Tunisia	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	7
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
69.30.198.146	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	2
107.150.32.58	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	2
74.91.17.181	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
109.67.228.35	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
82.145.209.76	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1

04-10-2016-02:04:08 to 04-10-2016-03:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
65.55.210.151	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.30.24.222	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-10-2016-02:04:08 to 04-10-2016-03:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
199.115.117.199	147.237.77.216	United States	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
88.204.187.90	147.237.77.235	Kazakstan	sviva.idf.il	ET SCAN NMAP -f -sS	2
112.64.185.123	147.237.72.166	China	aka.idf.il	GPL SCAN nmap TCP	2
88.204.187.90	147.237.77.235	Kazakstan	sviva.idf.il	ET SCAN NMAP -sS window 2048	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
88.204.187.90	147.237.77.235	Kazakstan	sviva.idf.il	ET SCAN NMAP -sS window 4096	2
162.248.100.195	147.237.0.200	United States	m4u.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
162.248.100.195	147.237.0.19	United States	madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1

04-10-2016-02:04:08 to 04-10-2016-03:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3740
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1983
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	SYN Attack		reject	1116
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	548
195.60.232.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	260
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
217.78.62.175	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	30
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	29
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	22
197.15.9.10	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
109.67.228.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
46.19.86.170	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	19
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.78	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	14
83.130.126.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
109.65.106.134	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
46.19.85.73	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.183.96.27	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
81.137.247.232	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
109.253.130.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
81.137.247.232	United Kingdom	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
176.228.130.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.169.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.52.128.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.157.142.102	Denmark	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
108.245.162.18	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
197.16.128.79	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
41.251.32.23	Morocco	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.65.106.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
105.154.115.82	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
178.255.215.87	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.180.105.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.80.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
197.164.191.62	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.220	Israel	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
197.28.23.57	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

04-10-2016-02:04:08 to 04-10-2016-03:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	72
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	68
195.60.232.57	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 195.60.232.57	Block	30
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	10
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	7
31.184.236.104	Russian Federation	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	6
149.202.239.134	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	6
149.202.239.135	France	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1283-en/dover.aspx parameter PageNum	Block	6
31.184.236.104	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.184.236.104	Block	5
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
197.15.9.10	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.15.9.10	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	3
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.110.7.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.140.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
54.210.18.124	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
208.115.125.36	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
77.75.76.160	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/34/	Block	1
149.202.239.135	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Distributed PHP Attempt	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/links.asp	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/2616.jpg	Block	1
107.150.46.37	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.tt782.com/	Block	1
54.210.18.124	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
217.69.133.243	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mail/kapats	Block	1
81.218.154.78	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.13	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.65.231	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
197.15.9.10	Tunisia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/cgi-bin/le_check_v3.exe	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1
62.210.148.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/trackback/	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
157.55.39.65	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19190-he/dover.aspx‚ƒ ƒ„,,¯ƒλ€Š„,¿„ƒ‚'¨'½¬,,Š€λƒ„,,¯ƒλ€Š„,¿„ƒ'½¬,,Š€λƒ„,,¯ƒλ€Š„,¿ ,½¬,,Š€λƒ¿¬,,Š€λƒ„,,¯ƒ‚'™½¬,,Š	Block	1
83.130.126.139	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/forms.asp	Block	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
37.26.149.206	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
197.16.128.79	Tunisia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
69.30.198.146	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.tt985.com/	Block	1
149.202.239.134	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1

04-10-2016-02:04:08 to 04-10-2016-03:04:08