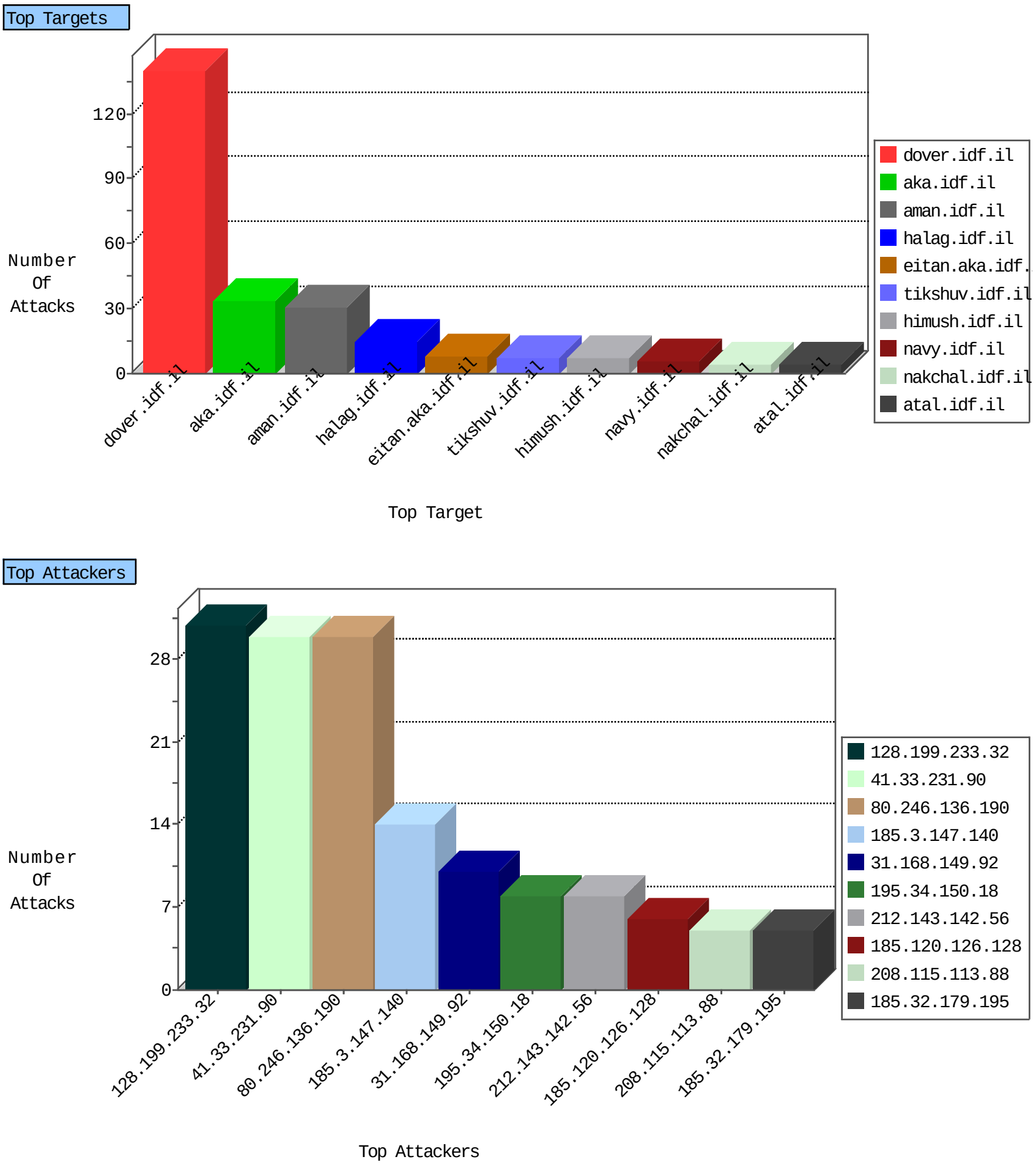
02-26-2016-02:04:01 to 02-26-2016-03:04:01

IDF Under Attack
Daily Report



02-26-2016-02:04:01 to 02-26-2016-03:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.36	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	115
42.112.10.89	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
59.29.207.55	Korea, Republic of	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
42.112.10.85	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
42.112.10.92	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
42.112.10.66	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
42.112.10.87	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
42.112.10.93	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
42.112.10.75	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.130.5.179		147.237.8.50	e.tikshuv.idf.i	Block_Udp_All_Nets	drop	1
42.112.10.88	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
42.112.10.84	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

02-26-2016-02:04:01 to 02-26-2016-03:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.135.189.103	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
51.255.51.70	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
157.55.39.92	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
151.80.31.151	Italy	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

02-26-2016-02:04:01 to 02-26-2016-03:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
80.246.133.214	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
128.199.233.32	147.237.72.166	Singapore	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
81.27.85.27	147.237.76.39	United Kingdom	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 3072	1
204.101.135.203	147.237.76.201	Canada	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
115.182.17.13	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
202.169.54.2	147.237.77.233	Indonesia	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1

02-26-2016-02:04:01 to 02-26-2016-03:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
128.199.233.32	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	30
185.3.147.140	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
80.246.136.190	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.246.136.190	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
31.168.149.92	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
185.120.126.128		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.190	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
80.246.136.190	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
185.32.179.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
58.8.120.133	Thailand	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
31.168.149.92	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
109.65.56.174	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
199.30.24.167	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.176.55.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.190.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.136.190	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
61.135.189.103	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
40.77.167.10	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
172.58.216.30	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
40.77.167.83	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
41.33.26.226	Egypt	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	2
141.212.122.203	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.136	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.62.53.168	Russian Federation	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.195	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.70	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.130.249.230	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
188.120.154.49	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
159.253.147.227	Netherlands	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.26.149.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.137	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.66.43.110	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.3.147.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.201	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.22.134.216	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.71	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
190.93.249.134	Costa Rica	147.237.76.38	e.e.meitav.idf.il	drop	First packet isn't SYN	drop	1
159.253.147.227	Netherlands	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.138	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.125.71.74	China	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
45.79.168.168		147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.202	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.39.222.159	Netherlands	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.130	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1

02-26-2016-02:04:01 to 02-26-2016-03:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	5
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
186.202.150.247	Brazil	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 186.202.150.247	Block	3
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.81.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
204.79.180.252	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
178.255.87.242	United Kingdom	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
91.196.50.33	Poland	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	1
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
199.30.25.178	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
125.209.235.185	Korea, Republic of	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
207.46.13.180	United States	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31/	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
185.3.147.140	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
98.27.229.138	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
204.79.180.162	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jeninkilled/stn	Block	1
66.249.81.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.167.29	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
185.49.14.190	Poland	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
109.67.146.3	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resource/userfollowresource/create/	Block	1
204.79.180.192	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.107	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
89.248.174.4	Netherlands	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
40.77.167.37	United States	147.237.72.166	aka.idf.il	Unknown Parameter c in www.aka.idf.il/miluim/templates/inner.asp	None	1
185.49.14.190	Poland	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on testp2.czar.bielawa.pl/testproxy.php	Block	1
116.66.197.233	Nepal	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.69.26	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
204.79.180.244	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
174.129.237.157	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
89.248.174.4	Netherlands	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
65.55.212.72	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
125.209.235.184	Korea, Republic of	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1

02-26-2016-02:04:01 to 02-26-2016-03:04:01