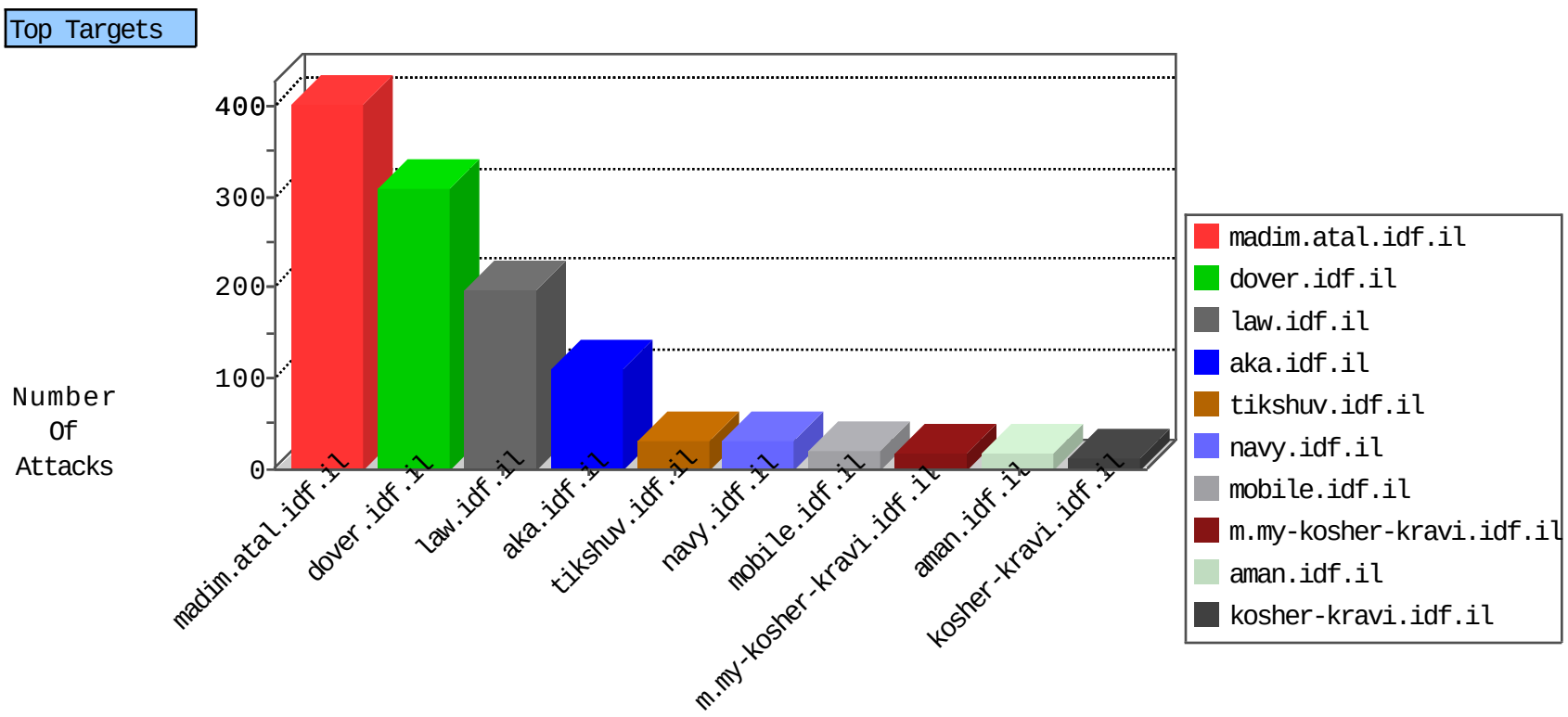
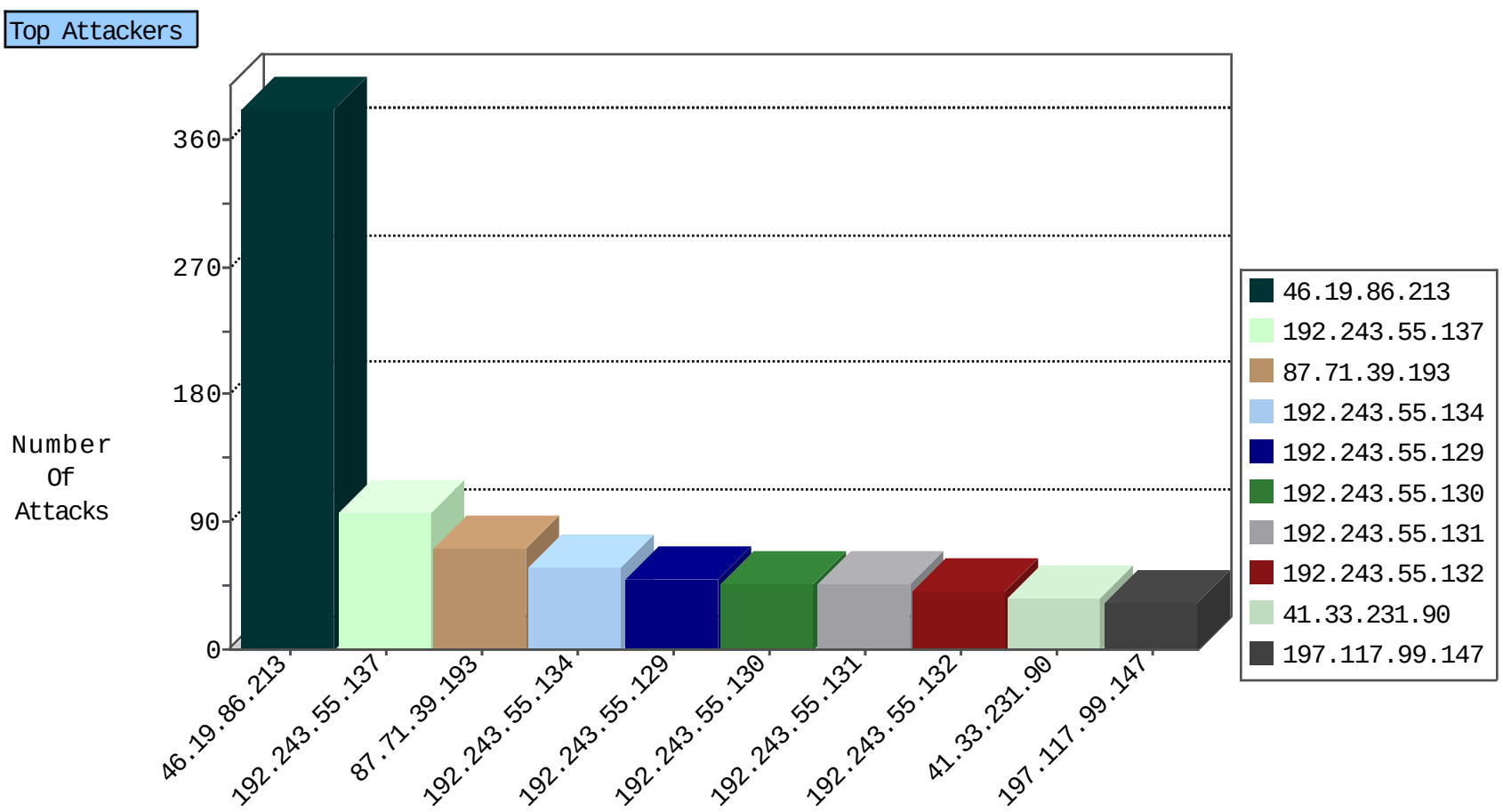
02-20-2016-09:04:01 to 02-20-2016-10:04:01

IDF Under Attack Daily Report



Top Target



Top Attackers

02-20-2016-09:04:01 to 02-20-2016-10:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.54.237	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
182.185.215.134	Pakistan	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	3
182.133.103.178	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
112.121.190.17	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
118.165.2.55	Taiwan	147.237.76.38	e.e.meitav.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
182.133.103.178	China	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
112.121.190.69	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
182.133.103.178	China	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
112.121.190.9	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
182.133.103.178	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
112.121.190.70	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
182.133.103.178	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
112.121.190.10	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
112.121.190.71	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

02-20-2016-09:04:01 to 02-20-2016-10:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.107.215	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
213.57.42.100	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	5
151.80.44.115	Italy	147.237.72.156	aman.idf.il	C1000106: HTTP: majestic bot	Block	2
151.80.41.169	Italy	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	2
151.80.44.115	Italy	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	2
84.108.94.232	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
151.80.41.169	Italy	147.237.76.42	refuah.idf.il	C1000106: HTTP: majestic bot	Block	2
151.80.41.169	Italy	147.237.77.176	matpash.idf.il	C1000106: HTTP: majestic bot	Block	2
66.249.81.199	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
151.80.41.169	Italy	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	2
66.249.81.202	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
66.249.81.199	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1

02-20-2016-09:04:01 to 02-20-2016-10:04:01

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
174.37.194.144	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sA (2)	2
185.110.132.54	147.237.76.201		e.atal.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
94.190.111.182	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.54	147.237.76.176		test.ncore.idf.il	ET SCAN Potential SSH Scan	1
94.190.111.182	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.54	147.237.76.34		yohalan.idf.il	ET SCAN Potential SSH Scan	1
94.190.111.182	147.237.76.197	Russian Federation	e.himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
94.190.111.182	147.237.76.177	Russian Federation	ncore.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
94.190.111.182	147.237.76.147	Russian Federation	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
94.190.111.182	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN Potential SSH Scan	1
118.165.2.55	147.237.76.86	Taiwan	navy.idf.il	ET SCAN Potential SSH Scan	1
94.190.111.182	147.237.72.217	Russian Federation	e.idf.il	ET SCAN Potential SSH Scan	1
94.190.111.182	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN Potential SSH Scan	1
94.190.111.182	147.237.72.14	Russian Federation	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
94.190.111.182	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.54	147.237.76.197		e.himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
94.190.111.182	147.237.77.74	Russian Federation	law.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.54	147.237.76.147		chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
94.190.111.182	147.237.76.201	Russian Federation	e.atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
94.190.111.182	147.237.76.196	Russian Federation	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
94.190.111.182	147.237.76.148	Russian Federation	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
94.190.111.182	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sA (2)	1
94.190.111.182	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Potential SSH Scan	1
94.190.111.182	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN Potential SSH Scan	1
197.117.99.147	147.237.77.216	Algeria	dover.idf.il	INDICATOR-COMPROMISE c99shell.php command request - sql	1
94.190.111.182	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN Potential SSH Scan	1
94.190.111.182	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1

02-20-2016-09:04:01 to 02-20-2016-10:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.71.39.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
87.71.39.193	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.120.73.244	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
104.148.71.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
104.148.71.83	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
104.148.71.90	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
185.3.144.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.137	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.130	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
2.54.128.72	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.137	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.7.215	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.132	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.132	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.129	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.142.68.174	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4

02-20-2016-09:04:01 to 02-20-2016-10:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.213	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.213	Block	243
46.19.86.213	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	102
46.19.86.213	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.86.213	Block	36
197.117.99.147	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.117.99.147	Block	30
208.115.111.72	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.111.72	Block	6
176.13.18.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	3
2.54.31.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
17.138.56.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.56.26	Block	3
66.249.83.155	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
207.46.13.193	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/captcha.ashx	Block	1
37.142.189.87	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
193.136.33.224	Portugal	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
141.212.122.160	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
182.185.215.134	Pakistan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
157.55.39.90	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.117.0.220	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19142-en/dover	Block	1
79.180.62.51	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.180.62.51	Block	1
46.19.86.213	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
197.117.99.147	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/Ø·	Block	1
157.55.39.134	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/navy/navy/default.aspx	Block	1
66.249.73.138	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list2005c.htm	Block	1
217.69.133.241	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/newsflash/newsflash.aspx/	Block	1
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	1
85.64.159.66	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
46.19.86.213	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
207.46.13.189	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.159	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.73.147	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
37.142.189.87	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
217.69.133.247	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/contactus/contactus.aspx/	Block	1
193.136.33.224	Portugal	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
91.200.12.24	Ukraine	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/fckeditor/_whatsnew.html	Block	1

02-20-2016-09:04:01 to 02-20-2016-10:04:01