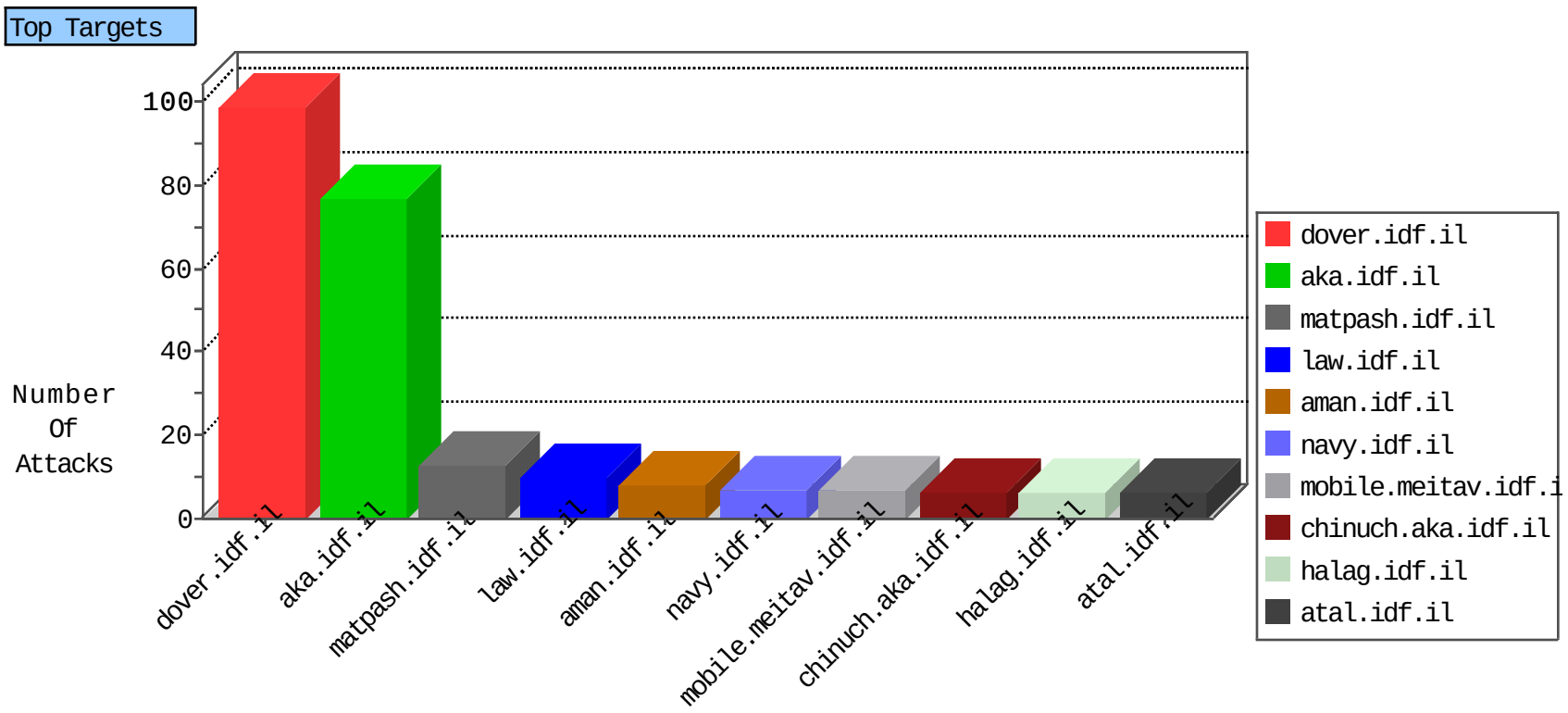
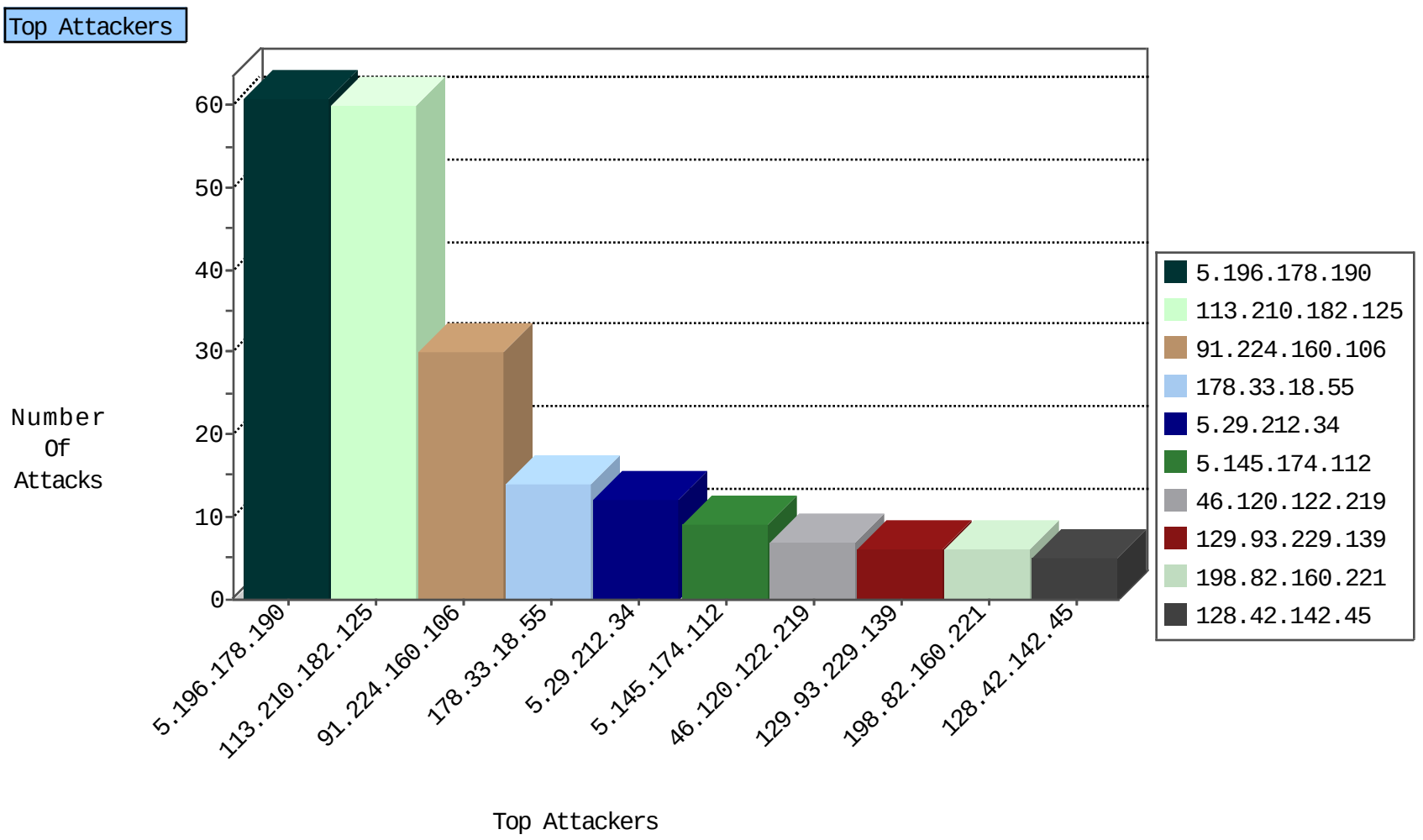
09-12-2016-03:04:01 to 09-12-2016-04:04:01

IDF Under Attack
Daily Report





09-12-2016-03:04:01 to 09-12-2016-04:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
202.171.186.156	Australia	147.237.77.216	dover.idf.il	ICMP-Frag-Needed-Storm	drop	3
129.22.150.78	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	2
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.117.226.180	Canada	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
120.132.50.135	China	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	1
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
165.230.49.118	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
131.179.150.72	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
141.22.213.34	Germany	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
179.99.200.39	Brazil	147.237.77.74	law.idf.il	block-sp-traf1	forward	1
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-12-2016-03:04:01 to 09-12-2016-04:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.145.174.112	Spain	147.237.77.176	matpash.idf.il	C1000016: HTTP: administrator in URI	Permit	9
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
69.50.221.6	United States	147.237.77.74	law.idf.il	C1000016: HTTP: administrator in URI	Permit	1
69.50.221.6	United States	147.237.77.74	law.idf.il	C1000018: HTTP: access to administrator/index.php -> Quarantine	Permit	1
94.102.49.190	Netherlands	147.237.0.19	madim.atal.idf.i	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-12-2016-03:04:01 to 09-12-2016-04:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	4
91.224.160.106	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
46.120.122.219	147.237.76.147	Israel	chinuch.aka.idf.il	Xenu Link Sleuth User Agent	2
91.224.160.106	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN Potential SSH Scan	1
178.33.18.55	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Poison Null Byte	1
91.224.160.106	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.77.61	United Kingdom	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
5.189.180.240	147.237.77.227	Germany	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.76.176	United States	test.ncore.idf.il	ET DROP Dshield Block Listed Source	1
91.224.160.106	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.77.233	United Kingdom	atal.idf.il	ET SCAN NMAP -sS window 1024	1
97.105.173.114	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	1

09-12-2016-03:04:01 to 09-12-2016-04:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
113.210.182.125	Malaysia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	34
5.29.212.34	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
113.210.182.125	Malaysia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
113.210.182.125	Malaysia	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.196.178.190	France	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
5.196.178.190	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
66.249.66.75	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.196.178.190	France	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
5.196.178.190	France	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
5.196.178.190	France	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
5.196.178.190	France	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
2.55.129.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
113.210.182.125	Malaysia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
5.196.178.190	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
5.196.178.190	France	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
5.196.178.190	France	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
113.210.182.125	Malaysia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.196.178.190	France	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
5.196.178.190	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
5.196.178.190	France	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
5.196.178.190	France	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
5.196.178.190	France	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
5.196.178.190	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
5.196.178.190	France	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
5.196.178.190	France	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
5.196.178.190	France	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
5.196.178.190	France	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
5.196.178.190	France	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
37.26.149.229	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
141.212.122.70	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
139.162.37.147	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
178.33.18.55	France	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
141.212.122.67	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
128.232.110.28	United Kingdom	147.237.0.35	akaws.idf.il	drop		drop	1
79.178.193.128	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
5.196.178.190	France	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.73	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
179.99.200.39	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.68	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
128.232.110.28	United Kingdom	147.237.77.235	sviva.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
85.65.9.199	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.74	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.65	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
31.168.172.137	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.69	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
128.232.110.28	United Kingdom	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
85.65.9.199	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.84	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-12-2016-03:04:01 to 09-12-2016-04:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.139.117.237	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	2
178.33.18.55	France	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 178.33.18.55	Block	1
68.180.229.190	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1806-he/dover.aspx	Block	1
66.249.66.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/mobile/main/giyus/general.aspx	Block	1
178.33.18.55	France	147.237.72.166	aka.idf.il	Unknown HTTP Request Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]„.ûZêôùSìiL×[[#24]]‡[[#26]]Ö ^	Block	1
178.33.18.55	France	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL ¸[[#20]]¸	Block	1
66.249.66.232	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/smalim/showbig.aspx	Block	1
37.26.149.221	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
178.33.18.55	France	147.237.72.166	aka.idf.il	Multiple Malformed URL from 178.33.18.55	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
180.76.15.137	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
178.33.18.55	France	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
66.249.79.59	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
41.254.9.211	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1115-ar/dover.aspx'	Block	1
178.33.18.55	France	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 178.33.18.55	Block	1
79.177.71.152	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/contact/contact.asp	Block	1
207.46.13.113	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18774-en/dover...for	Block	1
178.33.18.55	France	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 1	Block	1
68.180.229.181	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
46.120.122.219	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized Method HEAD for www.chinuch.aka.idf.il/894-he/chinuch.aspx	None	1
178.33.18.55	France	147.237.72.166	aka.idf.il	NULL Character in Header Name at [[#0]]œ[[#0]]•[[#0]]/[[#0]]5À[[#18]][[#0]]	Block	1
178.33.18.55	France	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
66.249.66.177	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
178.33.18.55	France	147.237.72.166	aka.idf.il	Malformed URL ¸[[#20]]¸	Block	1
68.180.229.181	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
66.249.66.59	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/shared/usercontrols/navmenu/	Block	1
178.33.18.55	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/changelog.txt	Block	1
178.33.18.55	France	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
66.249.66.179	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/showpicture.asp	Block	1

09-12-2016-03:04:01 to 09-12-2016-04:04:01