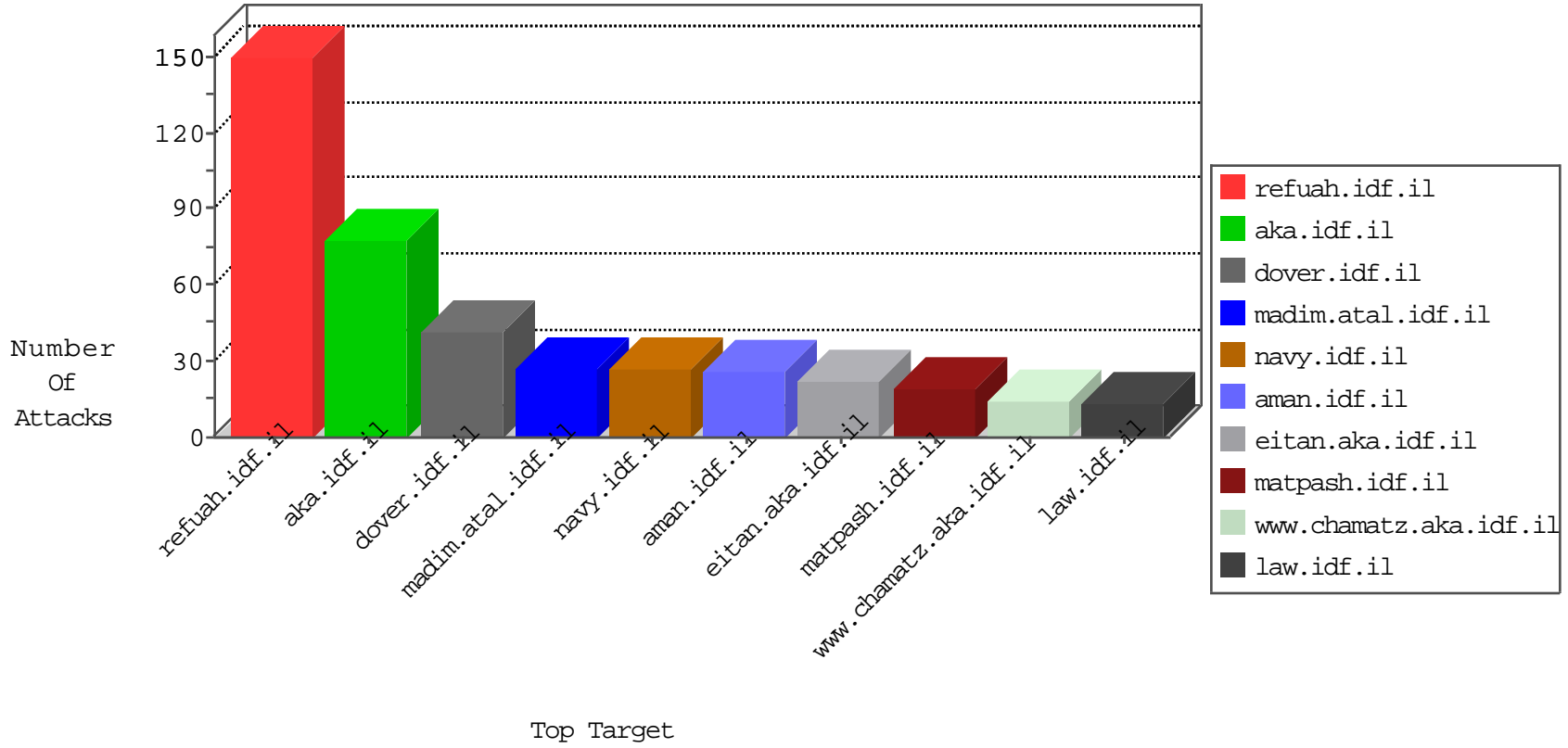


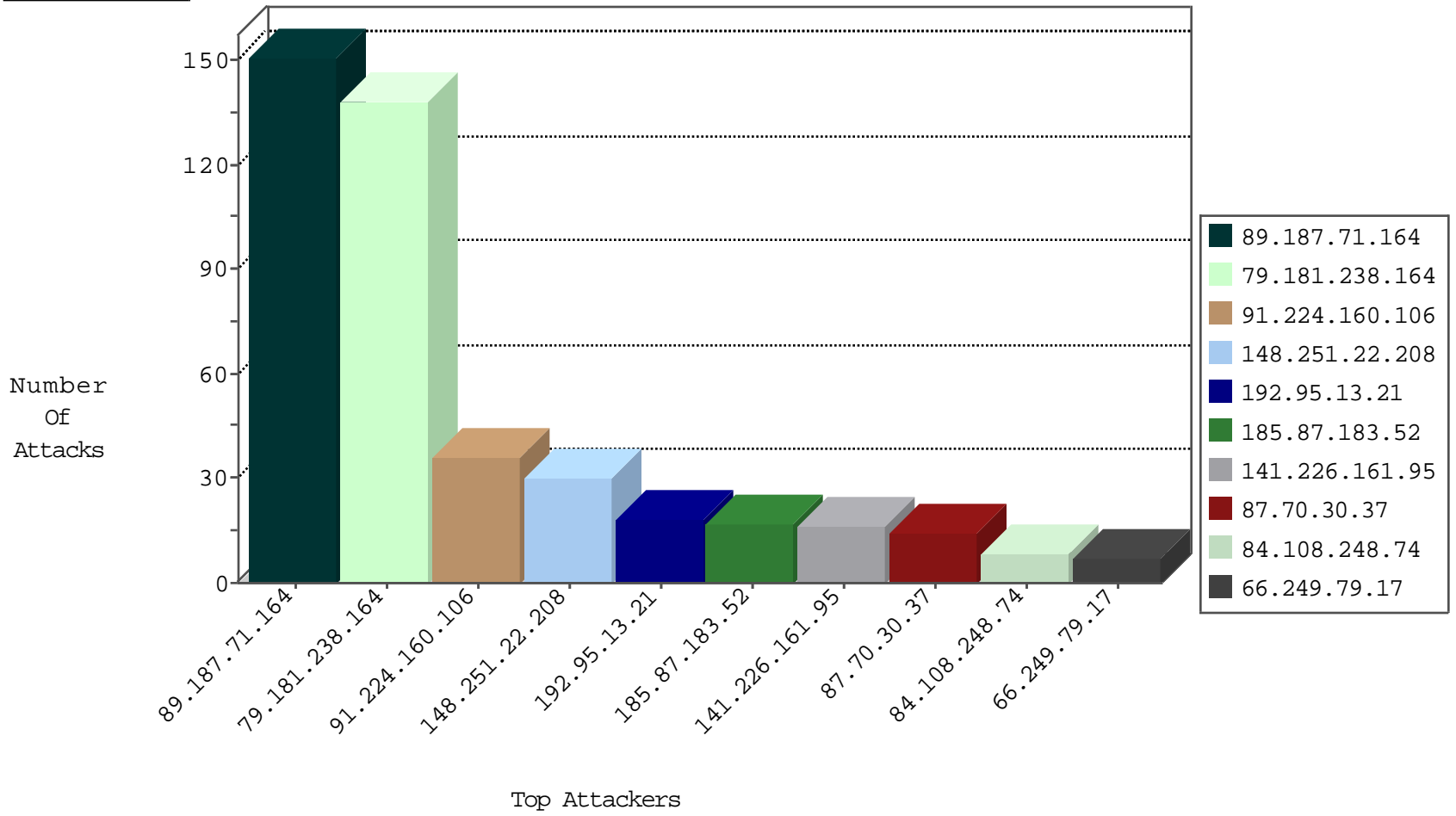
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	4
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
79.181.238.164	Israel	147.237.76.42	refuah.idf.il	Black List	drop	3
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.112	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
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.12	Canada	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
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.10.120.193	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	2
111.43.152.176	China	147.237.0.34	tikshuv.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
131.179.150.72	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
128.223.8.113	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
193.1.13.12	Ireland	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
36.110.147.66	China	147.237.77.74	law.idf.i	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
106.38.241.105	China	147.237.72.166	aka.idf.i	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
199.87.254.195	United States	147.237.77.74	law.idf.i	34161: ICMP: Communication with Destination Host is Administratively Prohibited (Code 10)	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.224.160.106	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	2
45.79.71.122	147.237.0.34	United States	tikshuv.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
91.224.160.106	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.8.14	Netherlands	e.orchot.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
212.224.109.175	147.237.77.227	Germany	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.154	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.154	147.237.76.177	China	noore.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.158	147.237.77.226	Sweden	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1
45.79.103.178	147.237.77.170	United States	maarachot.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
104.128.144.131	147.237.0.200	Canada	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
91.224.160.106	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.201	Netherlands	e.atal.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
163.172.169.150	147.237.0.15	United Kingdom	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	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	147.237.76.148	Netherlands	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.154	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.76.38	Canada	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
46.161.40.17	147.237.76.196	Russian Federation	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.0.200	Canada	m4u.idf.il	ET SCAN NMAP -f -sS	1
91.224.160.106	147.237.72.14	Netherlands	doover.idf.il(old)	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.181.238.164	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	134
141.226.161.95	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
192.95.13.21	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
89.187.71.164	United Kingdom	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
89.187.71.164	United Kingdom	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
89.187.71.164	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
89.187.71.164	United Kingdom	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
89.187.71.164	United Kingdom	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
89.187.71.164	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
84.108.248.74	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
89.187.71.164	United Kingdom	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
89.187.71.164	United Kingdom	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
89.187.71.164	United Kingdom	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
87.70.30.37	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
89.187.71.164	United Kingdom	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
89.187.71.164	United Kingdom	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
87.70.30.37	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
89.187.71.164	United Kingdom	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
89.187.71.164	United Kingdom	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
89.187.71.164	United Kingdom	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
66.249.79.17	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.187.71.164	United Kingdom	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
89.187.71.164	United Kingdom	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
89.187.71.164	United Kingdom	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.68.52.243	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
89.187.71.164	United Kingdom	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
89.187.71.164	United Kingdom	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
89.187.71.164	United Kingdom	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.94	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.65.94.22	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
89.187.71.164	United Kingdom	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
131.253.27.190	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
89.187.71.164	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
192.95.13.21	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
139.162.13.205	Singapore	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	3
148.251.22.208	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
5.22.134.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
148.251.22.208	Germany	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
148.251.22.208	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
187.61.110.201	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
197.36.126.238	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
148.251.22.208	Germany	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
79.177.247.147	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
148.251.22.208	Germany	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
148.251.22.208	Germany	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2

09-11-2016-02:04:00 to 09-11-2016-03:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.187.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.55.26.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.69.191	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
79.181.238.164	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.79.17	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1
94.102.49.190	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/robots.txt	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	1
68.180.228.41	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakchal.idf.il/1117-he/nakhal.aspx	Block	1
66.249.64.236	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	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
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1086-he/dover.aspx	Block	1
77.138.216.8	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.216.8	Block	1

09-11-2016-02:04:00 to 09-11-2016-03:04:00