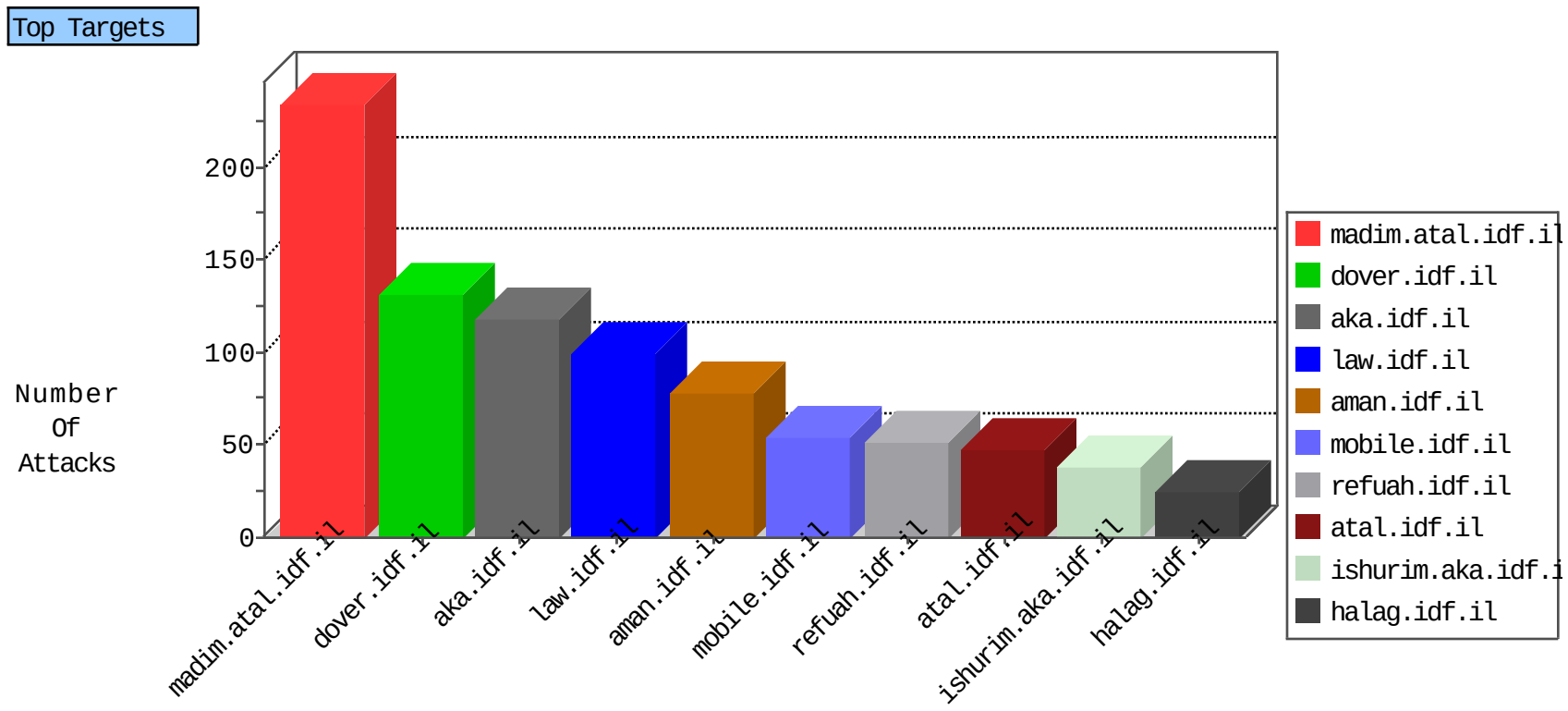
09-05-2016-16:04:00 to 09-05-2016-17:04:00

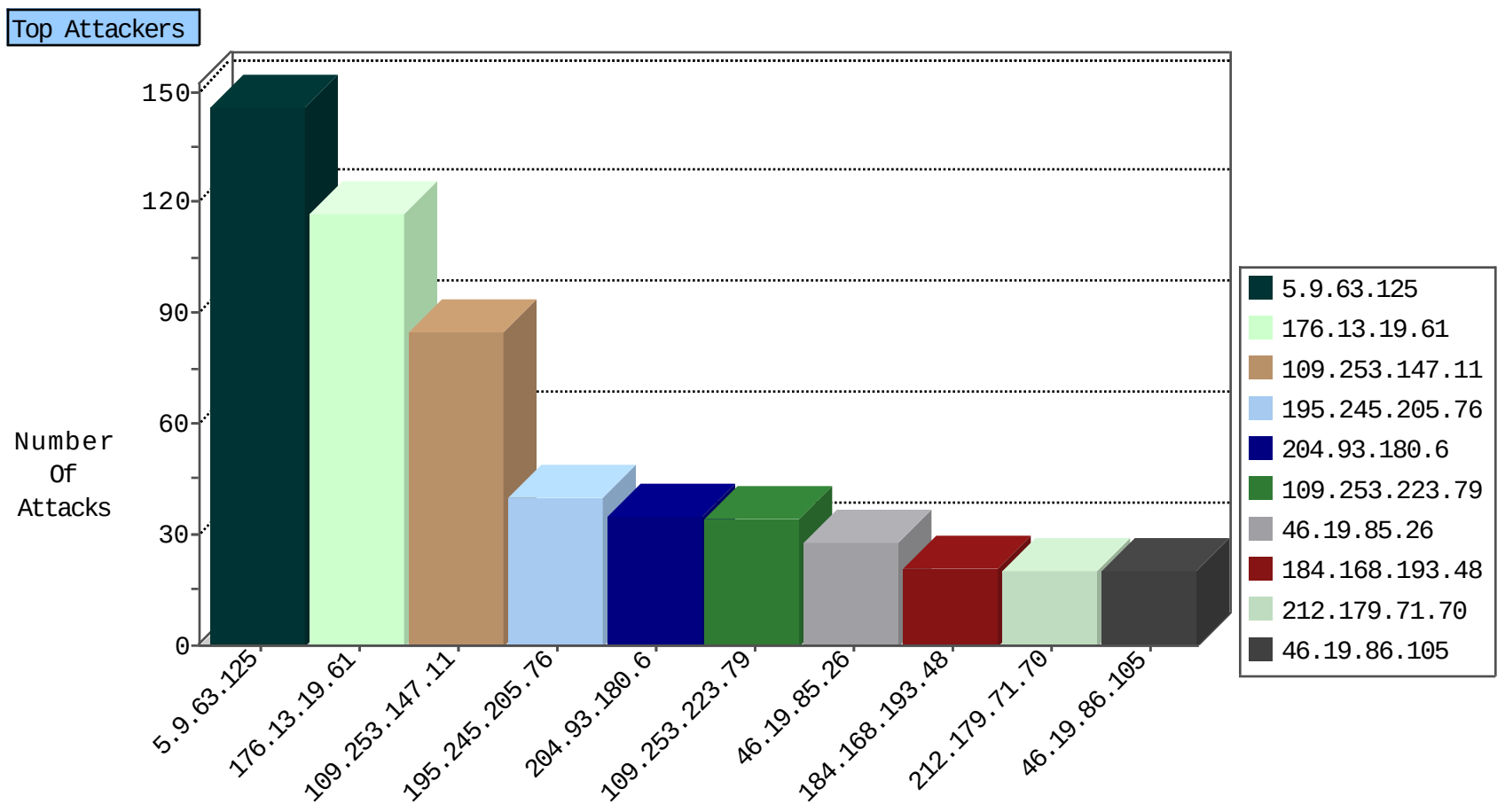
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-05-2016-16:04:00 to 09-05-2016-17:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.180.6	United States	147.237.77.74	law.idf.il	TCP Scan (vertical)	drop	155
2.53.190.101	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
123.59.59.52	China	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
109.236.84.10	Netherlands	147.237.76.177	ncore.idf.il	Black List	drop	1
222.186.135.44	China	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
79.180.172.254	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
89.248.168.21	Netherlands	147.237.76.177	ncore.idf.il	Black List	drop	1
89.248.168.21	Netherlands	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
217.23.9.123	Netherlands	147.237.76.34	yohalan.idf.il	Black List	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-05-2016-16:04:00 to 09-05-2016-17:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
184.168.193.48	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
187.17.109.54	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
176.10.104.240	Switzerland	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

09-05-2016-16:04:00 to 09-05-2016-17:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
184.168.193.48	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	15
187.17.109.54	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	6
195.245.205.76	147.237.76.44	Russian Federation	e.refuah.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	3
195.245.205.76	147.237.76.30	Russian Federation	himush.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	3
195.245.205.76	147.237.77.74	Russian Federation	law.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
195.245.205.76	147.237.8.14	Russian Federation	e.orchot.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
195.245.205.76	147.237.76.39	Russian Federation	mobile.meitav.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
195.245.205.76	147.237.77.233	Russian Federation	atal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
195.245.205.76	147.237.77.205	Russian Federation	prisha.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
195.245.205.76	147.237.8.50	Russian Federation	e.tikshuv.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
195.245.205.76	147.237.77.61	Russian Federation	e.cogat.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
195.245.205.76	147.237.0.200	Russian Federation	m4u.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
195.245.205.76	147.237.76.196	Russian Federation	e.sviva.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
84.109.45.143	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.76.42	Russian Federation	refuah.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
195.245.205.76	147.237.77.243	Russian Federation	mobile.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
82.166.21.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.76.31	Russian Federation	nakchal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
195.245.205.76	147.237.77.216	Russian Federation	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
80.246.139.207	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.72.156	Russian Federation	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
123.231.107.236	147.237.77.216	Sri Lanka	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.77.178	Russian Federation	e.matpash.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
195.245.205.76	147.237.8.46	Russian Federation	e.chinuch.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
79.180.3.30	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
103.207.36.84	147.237.8.24	Vietnam	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
66.249.76.75	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.77.19	Russian Federation	law-forum.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
101.200.75.131	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
195.245.205.76	147.237.0.33	Russian Federation	idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
46.19.86.33	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.76.200	Russian Federation	eitan.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
91.201.236.50	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
45.32.138.89	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
193.43.245.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.76.197	Russian Federation	e.himush.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
89.139.190.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.254.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
190.253.162.190	147.237.77.176	Colombia	matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
85.250.116.109	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.203.240.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.93.84.77	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	1
163.172.238.44	147.237.0.34	United Kingdom	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
81.218.158.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
147.236.232.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.210.86	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.232.98.38	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
195.245.205.76	147.237.77.121	Russian Federation	e.navy.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
195.245.205.76	147.237.8.45	Russian Federation	e.eitan.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1

09-05-2016-16:04:00 to 09-05-2016-17:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.85.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
212.179.71.70	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	20
184.168.27.33	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
109.253.223.79	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	14
46.19.86.67	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.105	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
109.253.223.79	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
5.9.63.125	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
109.253.223.79	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
84.110.177.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
5.9.63.125	Germany	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
84.110.177.160	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
5.9.63.125	Germany	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
5.9.63.125	Germany	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.86.105	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
5.9.63.125	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
5.9.63.125	Germany	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
5.9.63.125	Germany	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
95.86.88.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
195.60.235.57	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.19.85.200	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
87.70.247.170	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.85.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.9.63.125	Germany	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
5.9.63.125	Germany	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
5.9.63.125	Germany	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.85.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
5.9.63.125	Germany	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
5.9.63.125	Germany	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
109.253.202.196	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.231.227	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.106.184.160	Germany	147.237.77.233	atal.idf.il	drop	SAM rule	drop	6
46.19.85.229	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.161	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.53.51.235	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.178	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.229	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.161	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.141.186	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.9.63.125	Germany	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
5.9.63.125	Germany	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
5.9.63.125	Germany	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
5.9.63.125	Germany	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
5.9.63.125	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
5.9.63.125	Germany	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
5.9.63.125	Germany	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
5.9.63.125	Germany	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5

09-05-2016-16:04:00 to 09-05-2016-17:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.19.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	114
109.253.147.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
46.19.85.26	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
109.253.147.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
80.246.138.25	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	7
176.13.240.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.108.193.145	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
2.53.49.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.57.57.136	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/	Block	2
85.64.230.110	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
2.53.16.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.69.83	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/18205.pdf	Block	1
37.142.10.4	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
46.120.38.133	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
99.236.4.63	Canada	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
2.53.51.235	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.180.29.46	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
213.151.35.212	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1
66.249.69.97	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/2/242.doc	Block	1
85.65.80.225	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
66.249.76.114	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
62.219.133.75	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
109.64.99.34	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
2.53.51.235	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
79.182.100.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.151.48.138	Israel	147.237.72.166	aka.idf.il	Unknown Parameter CatID in www.aka.idf.il/main/giyus/general/	None	1
66.249.69.119	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.19.85.83	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
109.253.202.196	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
85.65.165.192	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
66.249.79.147	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1315-he/refuah.aspx	Block	1
180.76.15.23	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9235-he/refuah.aspx	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
109.65.62.45	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
2.53.157.225	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
132.74.58.20	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/2/109372.pdf	Block	1
87.70.247.170	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
2.53.37.208	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
66.102.9.6	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
109.253.129.241	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 109.253.129.241	None	1
8.37.225.49	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
46.19.86.67	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
132.74.168.171	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/59635.pdf	Block	1
98.223.23.29	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1

09-05-2016-16:04:00 to 09-05-2016-17:04:00