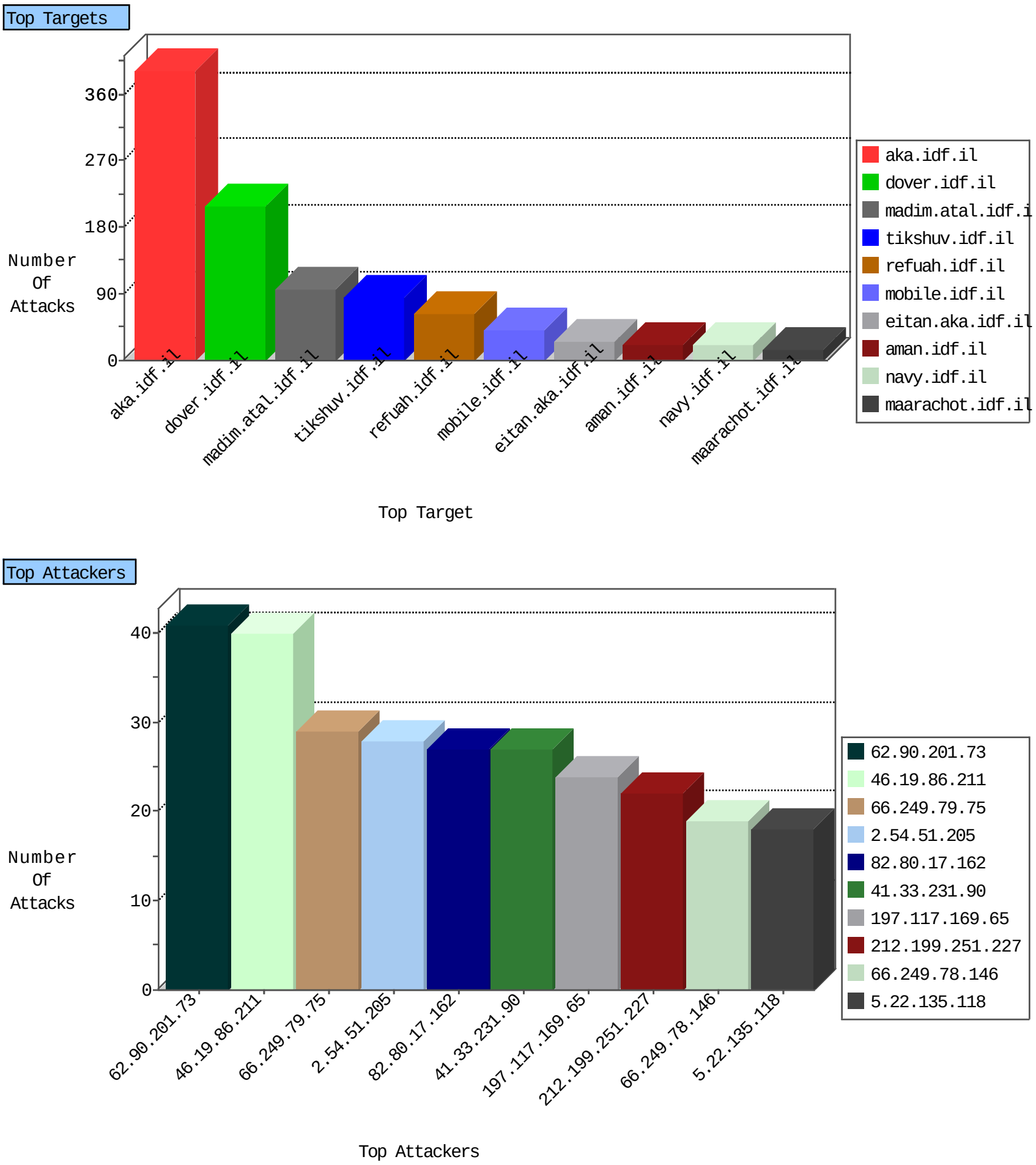
02-28-2016-13:04:03 to 02-28-2016-14:04:03

IDF Under Attack
Daily Report



02-28-2016-13:04:03 to 02-28-2016-14:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.117.169.65	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-product3	dest-reset	16
197.117.169.65	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	4
217.26.171.188	Moldova, Republic of	147.237.77.176	matpash.idf.il	L4 Source or Dest Port Zero	drop	3
222.74.220.19	China	147.237.76.176	test.ncore.idf.il	Invalid TCP Flags	drop	2
185.94.111.1		147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
217.26.171.188	Moldova, Republic of	147.237.76.176	test.ncore.idf.il	L4 Source or Dest Port Zero	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
188.138.102.50	Germany	147.237.8.50	e.tikshuv.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.33	Switzerland	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
182.222.150.205	Korea, Republic of	147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	1

02-28-2016-13:04:03 to 02-28-2016-14:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.172	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
212.179.42.225	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
37.26.147.219	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
213.57.169.246	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
212.235.64.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
151.80.31.153	Italy	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	2
51.255.65.32	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.69	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.154	Italy	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
66.249.64.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
84.108.9.171	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
51.255.65.28	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.150	Italy	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

02-28-2016-13:04:03 to 02-28-2016-14:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
149.88.12.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
37.26.148.197	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
125.212.232.146	147.237.76.198	Vietnam	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.164.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.6.117	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.179.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.165.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.20.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.218.165	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.98.57	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
46.19.86.239	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.23.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
40.78.62.82	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential SSH Scan	1
164.39.11.198	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.50.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.199	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.69.117	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.190.96	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.101.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.153	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.93.89	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.90.201.73	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.2.40	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.141.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-28-2016-13:04:03 to 02-28-2016-14:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
62.90.201.73	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
149.88.226.249	Israel	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	13
46.19.86.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.160.242	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.199.251.227	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
82.80.17.162	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
212.199.251.227	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
37.26.146.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.44	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	8
5.22.135.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.22.135.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.194.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.190.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.139.145	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
80.178.220.42	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.6.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.94.223.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.139.145	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.180.148.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.17.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
85.64.202.24	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
5.102.200.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.134.169	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	Invalid sequence number	monitor	6
176.13.22.164	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.24	Israel	147.237.72.166	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	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
31.210.188.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
81.218.55.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
80.179.114.27	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.147.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
46.19.85.100	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.180.3.172	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
62.219.191.47	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
185.3.147.151	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
66.249.64.3	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.23	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.136.92	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
82.80.137.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.49	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
193.104.77.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.74.123.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.62.121	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.22.135.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-28-2016-13:04:03 to 02-28-2016-14:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
66.249.79.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.75	Block	29
2.54.51.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
185.32.179.231	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	15
37.26.146.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
80.252.153.69	Russian Federation	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
80.252.153.69	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.252.153.69	Block	5
66.249.64.202	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	4
212.34.11.89	Jordan	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 212.34.11.89	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
197.117.169.65	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.117.169.65	Block	3
212.34.11.89	Jordan	147.237.77.216	dover.idf.il	Multiple Malformed URL from 212.34.11.89	Block	3
212.34.11.89	Jordan	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 212.34.11.89	Block	3
176.13.12.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
131.111.184.91	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 131.111.184.91	Block	2
131.111.184.91	United Kingdom	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	2
46.19.86.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.210.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/chinuch/klali/default.asp	None	2
79.176.54.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.146.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.131.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.181.29.187	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
131.111.184.91	United Kingdom	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1526-en/dover.aspx parameter searchText	Block	2
46.19.85.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
40.77.167.3	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/brothers/gallery/	None	1
93.146.78.164	Italy	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
66.249.69.30	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1745	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/brothers/faq/default.asp	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1384-he/dover.aspx	Block	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/giyus/kadatzhelp/	None	1
162.242.218.228	United States	147.237.77.216	dover.idf.il	Parameter Type Violation searchText in www.idf.il/1526-en/dover.aspx	Block	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;catID in www.aka.idf.il/giyus/forms/downloadform.asp	None	1
37.26.146.188	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.157.53	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Unknown Parameter reffer in www.aka.idf.il/ishurim/main	None	1
66.249.64.103	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;pageNum in aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
40.77.167.86	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/giyus/forms/	None	1
66.249.69.38	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1744	Block	1
95.86.84.70	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ved in www.aka.idf.il/main/sachar/klali.aspx	None	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;resized in www.aka.idf.il/edim/yoman/enlarge.asp	None	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;innerCatID in www.aka.idf.il/giyus/qanda/	None	1
174.62.245.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/navy/	Block	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in www.aka.idf.il/lomdim/tochen/	None	1
37.26.148.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.252.153.69	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
66.249.64.207	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on tikshuv.idf.il/main/giyus/general.aspx	Block	1

02-28-2016-13:04:03 to 02-28-2016-14:04:03