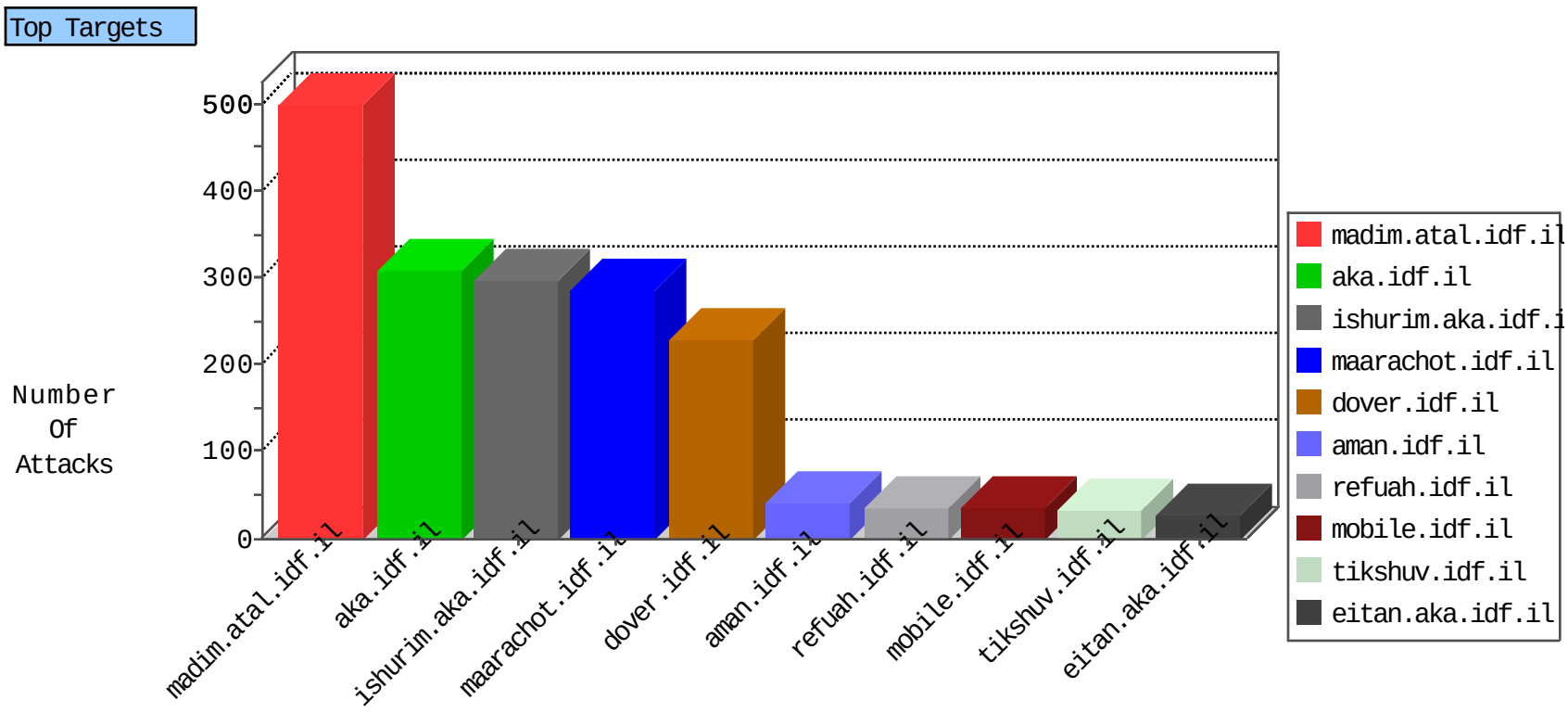
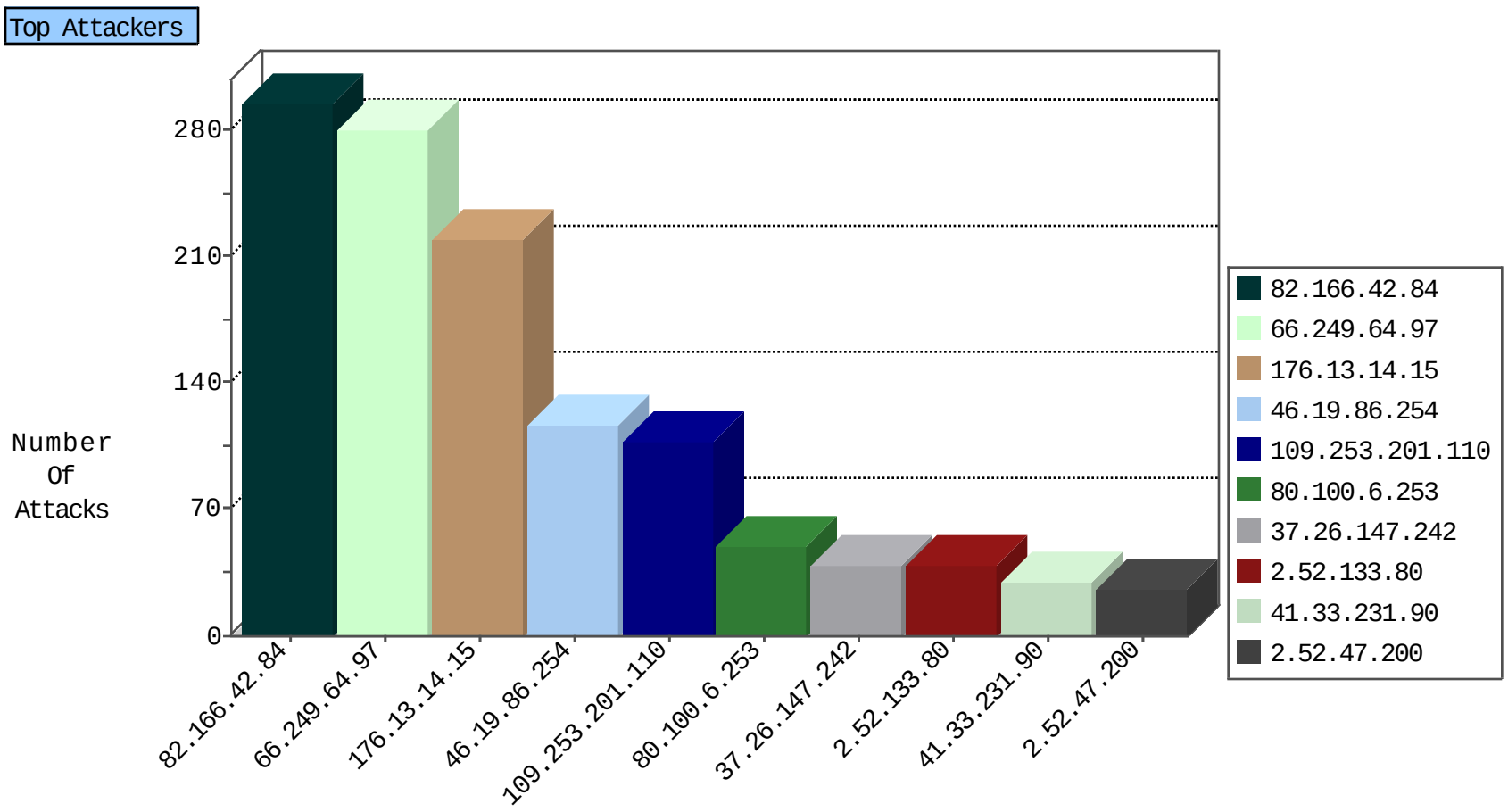
02-25-2016-16:04:08 to 02-25-2016-17:04:08

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-25-2016-16:04:08 to 02-25-2016-17:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
79.180.120.16	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
119.41.216.161	China	147.237.76.176	test.ncore.idf.il	Invalid TCP Flags	drop	2
119.41.216.161	China	147.237.76.177	ncore.idf.il	Invalid TCP Flags	drop	2
23.228.101.206	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
198.23.190.39	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
41.206.63.133	Kenya	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1
23.228.101.206	United States	147.237.77.243	mobile.idf.il	Block_Udp_All_Nets	drop	1
198.23.190.39	United States	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
23.228.101.206	United States	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
41.206.63.130	Kenya	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1
23.228.101.206	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
196.200.16.200	Kenya	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1
41.206.63.131	Kenya	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1

02-25-2016-16:04:08 to 02-25-2016-17:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.252.56	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
46.121.137.196	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
80.246.130.138	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.165.197.141	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
162.210.196.100	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
37.26.148.201	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
192.116.55.245	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
149.88.107.102	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
51.255.65.42	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
188.165.15.206	France	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.91	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

02-25-2016-16:04:08 to 02-25-2016-17:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	280
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
70.88.119.125	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.50	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
58.56.93.171	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.63	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.157.172	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.179.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
154.16.138.35	147.237.77.227	Mauritius	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
154.16.138.35	147.237.77.227	Mauritius	e.hamaz.idf.il	ET SCAN NMAP -f -sS	1
109.66.23.212	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.244.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.9.225	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.147.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.28	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.77.121	Sweden	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
154.16.138.35	147.237.77.227	Mauritius	e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
120.55.90.163	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1

02-25-2016-16:04:08 to 02-25-2016-17:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.166.42.84	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	295
80.100.6.253	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
79.183.140.242	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
2.54.179.8	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
81.218.190.43	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.133.80	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	12
176.13.18.238	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.28	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
2.52.44.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.27.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.47.200	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
2.52.47.200	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
62.0.237.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
45.219.124.197	Uruguay	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.253.214.218	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.85.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.179.46.16	Israel	147.237.76.197	e.himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
190.98.49.30	Suriname	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
2.52.133.80	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
5.43.194.54	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
2.52.133.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.65.191.110	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.137.5	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.52.165.95	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
31.168.154.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.133.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.219.137.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
37.26.147.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.138.98.154	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.133.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
62.219.163.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.160.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.148.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
79.180.148.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.142.231.229	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
185.3.147.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.100.6.253	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
5.29.139.113	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.106	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.143.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.172.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.47.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.162.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.213.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
134.249.53.96	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
46.19.86.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.144.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-25-2016-16:04:08 to 02-25-2016-17:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.14.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	219
46.19.86.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
109.253.201.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
37.26.147.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
46.19.85.15	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	6
79.182.30.246	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.182.30.246	Block	3
2.54.26.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.22.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.126.209.51	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
37.26.147.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.151	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/894-he/orchot.asp	Block	2
149.88.175.64	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
85.65.176.145	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
2.54.155.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
174.90.20.72	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
80.246.136.245	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.39	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
176.10.99.209	Switzerland	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
37.26.146.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
95.86.97.64	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/sip_storage/files/4/1904.pdf&sa=u&ved=0ahukewip3j3pk5plahwkqbqkhzrxdyyqfggymac&usg=afqjcngrru5bygo9uzugztsvirv0nj3hzw	Block	1
89.138.223.218	Israel	147.237.72.156	aman.idf.il	Multiple Malformed URL from 89.138.223.218	Block	1
66.249.69.11	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/scriptresource.axd	Block	1
46.19.86.106	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.41	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to chinuch.aka.idf.il/templates/general/general.aspx	Block	1
89.138.223.218	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Parameter Name ¯G¥¢¸¸¬pƤ\¬`PR1÷6D·„Ʊ™ ˜Dq]]#0[[″h—]]#8[[•¯¸¡˜ʺc·kכc†F¸e¡½;[[#31]][[#16]]‹Ls]]#11[[ה]]#25[[§[[#5]]¸¥S×?ע׀ʌM¨o'&¸d[[ב#30³»w,*ƒ&`4]]0#[[³´P×b÷]]ƥ3d„[[#19]]¨ה PXÞ YUu[[#6]],/[[½ƪœ#5]]1[[•´λ˜#15]]41#[[u‡]]ʺ¨ÿ`Ɒ¸sLλ½wi¸<s!	Block	1
37.26.148.231	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
125.209.150.50	Australia	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-ar/cogat.aspx	Block	1
89.138.223.218	Israel	147.237.72.156	aman.idf.il	NULL Character in URL Ÿc*¸s[[:#21l"]]81#[[l]]ƥ6j„y#mת4¨y^m]ƪa¨)ÿdo)¸‹bk„ת‌כ…f'q*+•Ÿw[[#11]]½[[#6]]0z¾‡¯–'98Ůzû u]cרעxr¬]]#28[[]]#0[[[[#27]]!„,f´&stp•'}vת7,ƒ¸[[˜כ#12[[ƥ~]]#6]]6#[[o]]	Block	1
89.138.223.218	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Name from 89.138.223.218	Block	1
66.249.64.48	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/2/105822.pdf	Block	1
82.166.140.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl95 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.85.39	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version __atuvs=56cf177bac80a2ce000; _pk_id.20.8afc=292321bc5cfba5e5.1450955687.2.1456412541.1456412541.; _pk_ses.20.8afc=*	Block	1
95.86.100.25	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/&sa=u&ved=0ahukewjntr_njjplahwbuhokhuekcpkqfggrmaq&usg=afqjcnhdhx85tdz_a0-eyy7o0ff9_7steg	Block	1
78.106.126.235	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
66.249.69.19	United States	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/robots.txt	Block	1
89.138.223.218	Israel	147.237.72.156	aman.idf.il	Multiple NULL Character in Header Name from 89.138.223.218	Block	1
46.19.86.187	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
89.138.223.218	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Query String ¯G¥¢¸¸¬pƤ\¬`PR1÷6D·„Ʊ™ ˜Dq]]#0[[″h—]]#8[[•¯¸¡˜ʺc·kכc†F¸e¡½;[[#31]][[#16]]‹Ls]]#11[[ה]]#25[[§[[#5]]¸¥S×?ע׀ʌM¨o'&¸d[[ב#30³»w,*ƒ&`4]]0#[[³´P×b÷]]ƥ3d„[[#19]]¨ה PXÞ YUu[[#6]],/[[½ƪœ#5]]1[[•´λ˜#15]]41#[[u‡]]ʺ¨ÿ`Ɒ¸sLλ½wi¸<s!	Block	1
79.182.30.246	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-ar/cogat.aspx	Block	1
89.138.223.218	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
89.138.223.218	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Value from 89.138.223.218	Block	1
66.249.64.53	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/111165.pdf	Block	1
46.19.85.39	Israel	147.237.77.216	dover.idf.il	Malformed URL __atuvc=1	Block	1
37.26.147.226	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.186.171.181	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
78.106.126.235	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
68.46.9.211	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
89.138.223.218	Israel	147.237.72.156	aman.idf.il	Multiple Unknown HTTP Request Method from 89.138.223.218	Block	1

02-25-2016-16:04:08 to 02-25-2016-17:04:08