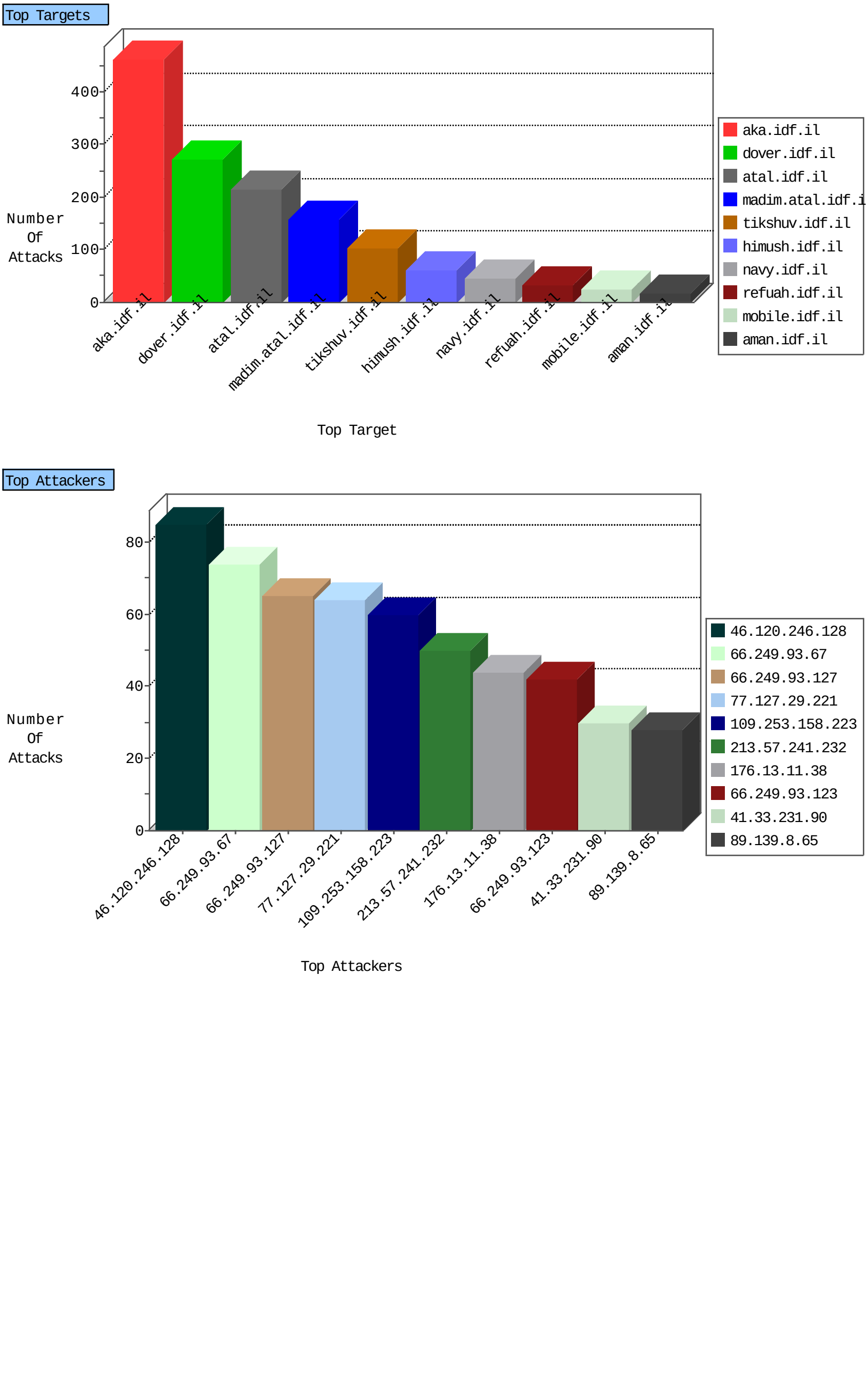
02-08-2016-20:04:04 to 02-08-2016-21:04:04

IDF Under Attack
Daily Report



02-08-2016-20:04:04 to 02-08-2016-21:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.44.127.199	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
128.194.131.235	United States	147.237.72.166	aka.idf.il	block-sp-traf1	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
74.91.28.59	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1

02-08-2016-20:04:04 to 02-08-2016-21:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-08-2016-20:04:04 to 02-08-2016-21:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
176.13.11.38	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
80.82.79.104	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.36.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.151.45.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
61.155.203.54	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.155.203.54	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.76.177	Sweden	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
46.151.52.161	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.3.147.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.191.106	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.4.254	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.135.175	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.198.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.107.135	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
79.181.38.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.47.237.95	147.237.76.147	France	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.155.203.54	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
193.109.199.196	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
54.67.38.74	147.237.76.31	United States	nakchal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
188.120.148.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.181	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
114.33.130.35	147.237.76.44	Taiwan	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.173.190.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-08-2016-20:04:04 to 02-08-2016-21:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.93.67	United States	147.237.77.233	atal.idf.il	drop		drop	45
66.249.93.127	United States	147.237.77.233	atal.idf.il	drop		drop	43
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
89.139.8.65	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	26
213.57.241.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
213.57.241.232	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
82.145.219.184	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
176.13.11.38	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
176.13.11.38	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
85.65.205.37	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
46.19.85.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
80.246.133.177	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
201.37.163.30	Brazil	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
46.116.26.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
213.140.59.136	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
5.102.254.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
109.65.127.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.93.67	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
66.249.93.67	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
5.28.173.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.93.127	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
79.180.28.240	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
66.249.93.127	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
66.249.93.67	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	7
185.32.179.167	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.100.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.51.29	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
37.46.38.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.66.202.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
105.155.231.205	Morocco	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	6
149.78.254.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
80.246.133.177	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.228.12.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.54.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.186.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.99.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.229.28.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.207.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.37.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.93.123	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.92	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
176.13.14.39	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
66.249.93.123	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.254.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	5
193.109.199.196	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.3.147.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

02-08-2016-20:04:04 to 02-08-2016-21:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.246.128	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	85
77.127.29.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	63
109.253.158.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
109.64.36.219	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 109.64.36.219	Block	10
37.26.147.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
46.19.86.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.52.54.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.3.144.62	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
94.230.86.31	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.136.99	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.120.125.60		147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	2
82.81.77.109	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
176.13.3.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.159.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.111.38.42	Israel	147.237.72.166	aka.idf.il	Malformed URL	Block	1
80.178.24.94	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
185.24.206.58	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.64.185.139	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
87.68.51.29	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
5.29.80.165	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.29.80.165	Block	1
201.37.163.30	Brazil	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.111.38.42	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name #dSKa2nÃ,"EÃŸ[[#17]][[#3]] Ã–YÃ" sOpÂ°Â²oÂ¹_>Q")cÂ¯b%Ã‡Â‹Â¡ÃŸÃ³Ã€[[#24]]lxm6Ã–ÂŒÂ»;Ã±IÂŽÃ´Â®Ã, [[#25]]Â?Ã¬BÃ³ÂšÃ¥[[#25]]Â£[[#22]]]L1Â¦Â?Â©zÃ¡Ã¤Â¦Â³[[#12]]BtÂ"ÃŠ [[#6]]1Â†P`Â³Â?Â¯AÃ°u[[#27]]Â§ÂšÃ¿/Ã•Ã«[[#5]]5ÂŠ Â¸[[#19]][[#28]]%X[[#17]][[#27]]miÂ–Â¹Â-[lt[[#20]]Ã„ Ã«[[#31]]w^Â¬[[#23]]QeÂ?`[[#17]]ÃµÂ,mÃ¸Â§2K Â†Ã©Ã™Â´Â–7Ot\Âµ<[[#15]] $ÃˆÃ¨^Ã¹NÃ°}DJf]MLÃªÂ Â,OÂ¡Â²Â›Ã¿vÃŒ Ã?'Ã¼[[#7]]vÂ?Ã¦!Â±'<MÂœÃ‰Ã?[[#7]]Â–ÃŒWÂ?Â¤[[#29]]Ã¦[[#0]]Â£Â›Ã© Ã¯Â¡S$Â¡Â¶Â„[RÂ¦ÂŒÃ†Ã¤Ã?[[#2]]Â‡b'Ã¸ [[#18	Block	1
77.126.60.147	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
157.55.39.75	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
46.120.180.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
95.86.119.232	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1300-he/navy.aspx&sa=u&ved=0ahukewividb45ujkahuhqw4khcl-by8qqoubcd4wcw&sig2=qdxm8ksa8nzbziyswec2uw&usg=afqjcngpx1u8pa04itbqoim7xaoax6qhqg	Block	1
84.111.38.42	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at Ã¾[[#2]]QgÂ'Ã }Â§1PÃ?Ã–Ã±Ã–7Â¿Ã¥]Ã¦Â¥Ã?HÃ¹Â?Â€?AÃ¬Â˜Ã"Ã‹[[#0]]Ã¹Ã•9*Ã¼Ã©Ã¾ÂŠÃ°ZKrÂªÂŠ [[#19]]Â?g[[#27]]6Ã"[[#4]]rfÂ†u@OPÂ¯Ã¤Ãƒ[[#27]]Ã³<Ãž[[#5]]Â, [[#17]]Ã½[[#0]]tÃšÃ?3Â»Ãµ%-d	Block	1
81.218.251.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/def	Block	1
185.32.179.167	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
87.69.197.188	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$42 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
5.29.80.165	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/×–×"	Block	1
208.80.194.26	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
84.111.38.42	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
157.55.39.100	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/military-police/	Block	1
104.227.56.19		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/documents.asp	Block	1
84.111.38.42	Israel	147.237.72.166	aka.idf.il	Too Many Headers per Request - 37 Headers	Block	1
109.253.139.174	Israel	147.237.72.166	aka.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1402-he/atal.aspx	Block	1
93.172.20.49	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
84.111.38.42	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method }Â¦PÃ˜dÂ¼Â†&Ã¿Ã?Â§Ã…RÃ„Â±uÂ?Ã–Â½;Ã¶[[#24]]Ã˜Ãž1[[#4]]Â‡Ã›ÂŒT+ÃªÂ“Ã±Ã¹ÂŽ-I•Â•Ã·+Â„J*ÃšÂŠÂ?ÂœÂŸÃœÂ¦[[#18]]mÃ°tÂ,YmPn(Ã¼Ã'Ã'Â‰[[#12]]!Ã¡$$Â§;nÂµÂ… EÃ¡ÃªÂ»G&%6\6[[#26]]Â®Ã-Â°Ã¡	Block	1
77.127.29.221	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 77.127.29.221	Block	1
50.253.2.217	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
84.111.38.42	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method }Â¦PÃ˜dÂ¼Â†&Ã¿Ã?Â§Ã…RÃ„Â±uÂ?Ã–Â½;Ã¶[[#24]]Ã˜Ãž1[[#4]]Â‡Ã›ÂŒT+ÃªÂ“Ã±Ã¹ÂŽ-I•Â•Ã·+Â„J*ÃšÂŠÂ?ÂœÂŸÃœÂ¦[[#18]]mÃ°tÂ,YmPn(Ã¼Ã'Ã'Â‰[[#12]]!Ã¡$$Â§;nÂµÂ… EÃ¡ÃªÂ»G&%6\6[[#26]]Â®Ã-Â°Ã¡ in URL	Block	1
194.90.66.9	Israel	147.237.72.166	aka.idf.il	Unknown Parameter _ in aka.idf.il/main/giyus/default.aspx	None	1
84.111.38.42	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
66.249.93.67	Israel	147.237.77.233	atal.idf.il	URL is Above Root Directory www.atal.idf.il/../../images/shared/menustrech.png	Block	1
94.185.83.100	Sweden	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on testp5.mielno.lubin.pl/testproxy.php	Block	1
84.111.38.42	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 1	Block	1

02-08-2016-20:04:04 to 02-08-2016-21:04:04