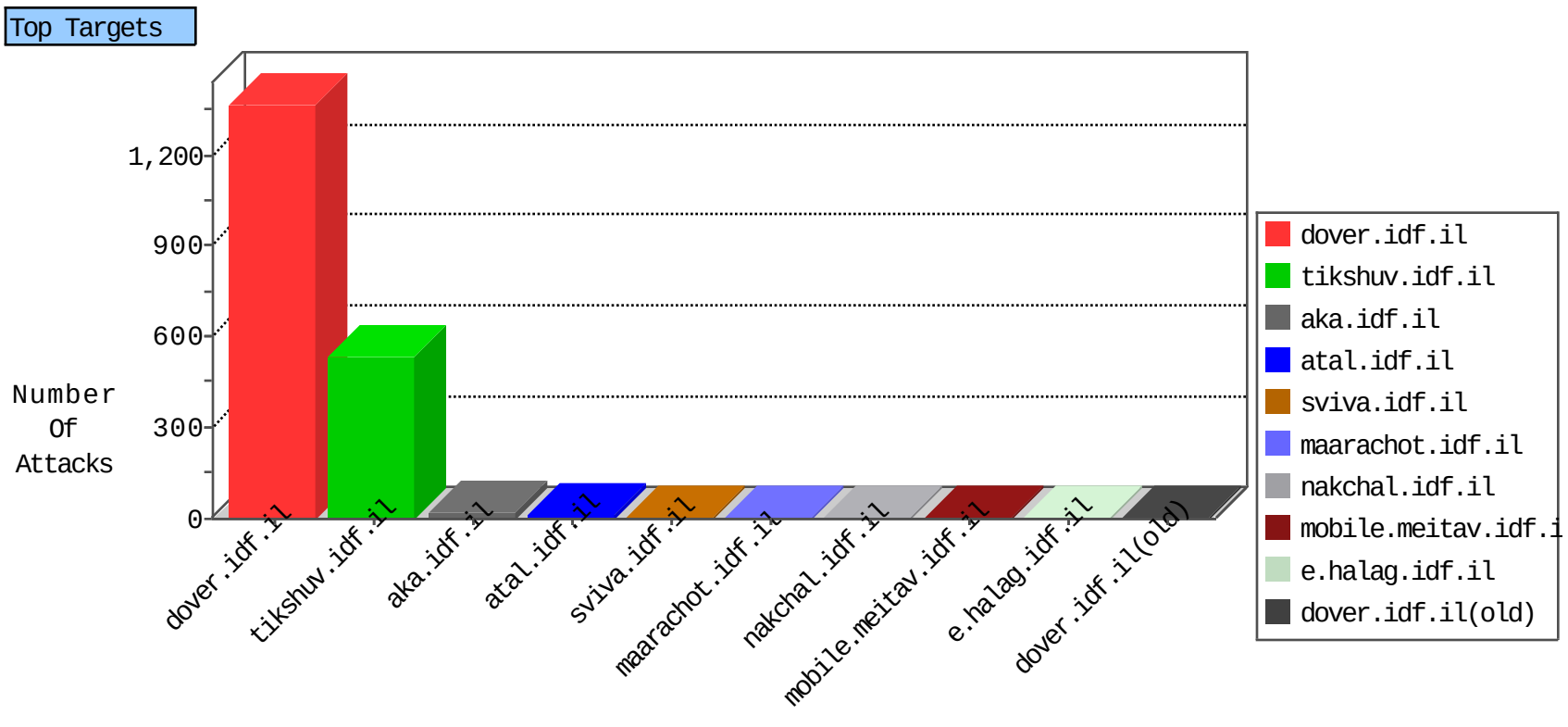
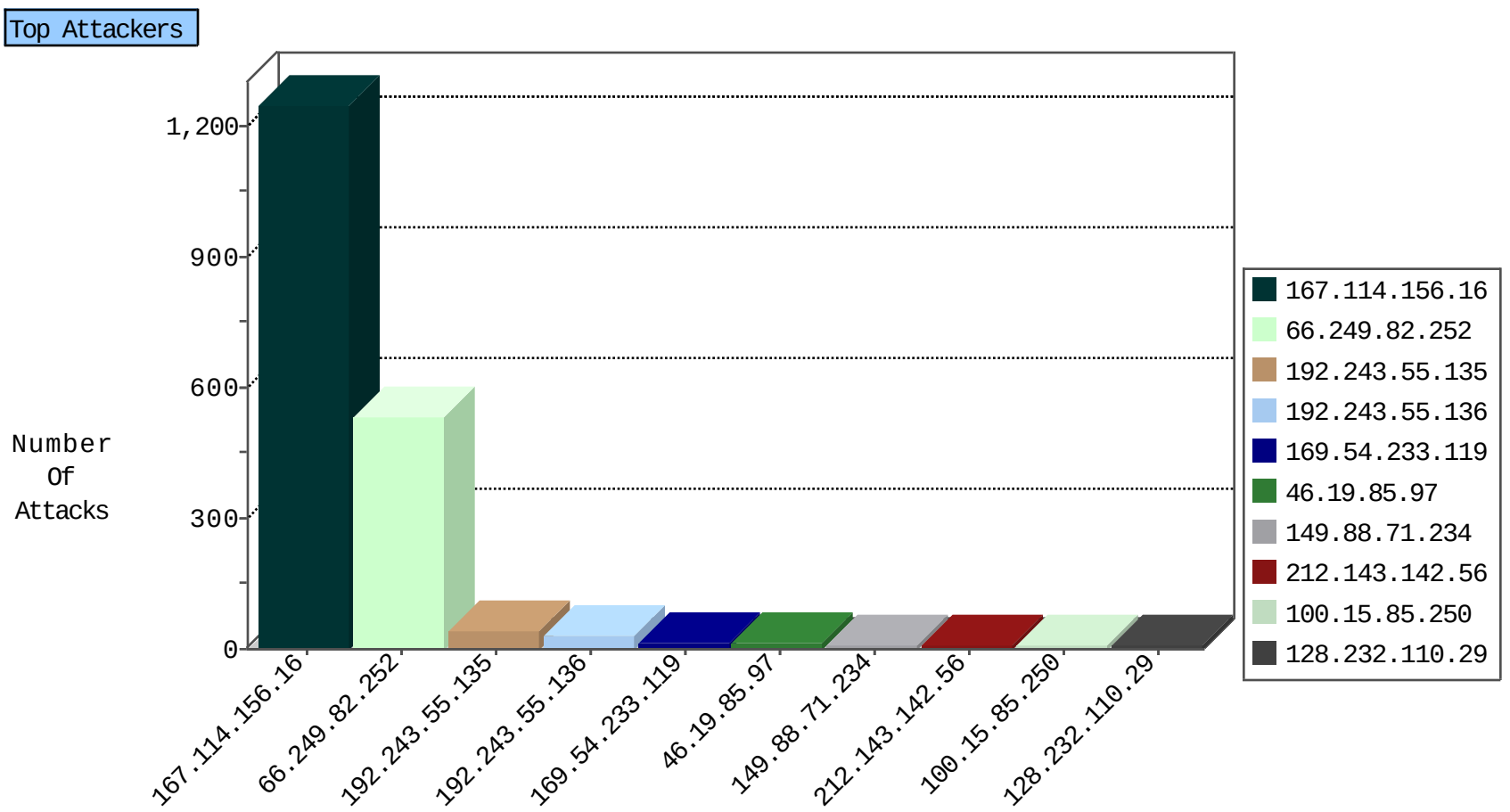
03-12-2016-05:04:00 to 03-12-2016-06:04:00

IDF Under Attack Daily Report





03-12-2016-05:04:00 to 03-12-2016-06:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4000
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
184.105.139.84	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
178.162.198.132	Germany	147.237.77.178	e.matpash.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1
184.105.247.236	United States	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.72	United States	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
94.102.49.206	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.100	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
178.162.198.132	Germany	147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	1
74.82.47.54	United States	147.237.77.205	prisha.idf.il	Block_Udp_All_Nets	drop	1
184.105.247.248	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.72	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.206	Netherlands	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.104	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.33	Switzerland	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
202.173.9.67	China	147.237.8.45	e.eitan.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.76	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.124	United States	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.33	Switzerland	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.206	Netherlands	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1

03-12-2016-05:04:00 to 03-12-2016-06:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.198	France	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

03-12-2016-05:04:00 to 03-12-2016-06:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.82.252	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	533
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
169.54.233.119	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
58.253.96.122	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.119	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
203.197.205.118	147.237.72.14	India	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1
169.54.233.119	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
202.71.25.29	147.237.77.235	India	sviva.idf.il	ET SCAN NMAP -f -sS	1
169.54.233.119	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
183.61.109.189	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
164.39.11.198	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.119	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
93.113.125.12	147.237.76.30	Romania	himush.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.119	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
169.54.233.119	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.139.54.71	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.119	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
58.253.96.122	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
218.246.0.97	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.119	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
58.253.96.122	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -f -sS	1
203.197.205.118	147.237.72.14	India	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
169.54.233.119	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
202.71.25.29	147.237.77.235	India	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
169.54.233.119	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
169.54.233.119	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
183.61.109.189	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
93.174.95.87	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
169.54.233.119	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
169.54.233.119	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.139.54.71	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.119	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.139.54.71	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

03-12-2016-05:04:00 to 03-12-2016-06:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
100.15.85.250	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.179.192.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
40.77.167.21	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.29	United Kingdom	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
37.46.39.234	Israel	147.237.76.39	mobile.meitav.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
82.165.135.208	Germany	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.161	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.15	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.94	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.232.110.29	United Kingdom	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
82.165.135.208	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
195.62.53.168	Russian Federation	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
128.232.110.29	United Kingdom	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
74.82.47.27	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.235	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
137.226.113.7	Germany	147.237.77.19	law-forum.idf.il	drop	SAM rule	drop	1
82.165.135.208	Germany	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
128.232.110.29	United Kingdom	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.27	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.243	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
137.226.113.7	Germany	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
82.165.135.208	Germany	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.88	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
64.114.255.114	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
184.105.139.76	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.252	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.160	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
82.165.135.208	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.15	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.87	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
128.232.110.29	United Kingdom	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1

03-12-2016-05:04:00 to 03-12-2016-06:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.82.94	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method "•wÝ[[#6]]½.ÿð²†ÍŸ¼ú–w)ýHb€ÒJÉ1[[#12]]g®§É[[#18]]ø·nÅdvš3ç[[#16]]Öˆ[[#31]][[#27]]*qK[JÂÎ„[[#15]]5^¥Ò¬[[#4]][[#3]]¼-C¥)ž³Gê³Êö›š¼¯<X˜Y+	Block	1
80.82.65.82	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.64.106	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method "•wÝ[[#6]]½.ÿð²†ÍŸ¼ú–w)ýHb€ÒJÉ1[[#12]]g®§É[[#18]]ø·nÅdvš3ç[[#16]]Öˆ[[#31]][[#27]]*qK[JÂÎ„[[#15]]5^¥Ò¬[[#4]][[#3]]¼-C¥)ž³Gê³Êö›š¼¯<X˜Y+ in URL	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
68.180.230.102	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 9	Block	1
128.232.110.28	United Kingdom	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.77	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
71.70.241.73	United States	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Malformed URL	Block	1
131.253.25.140	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name ú¬I-D0lÃ?È`öLÊS¬Å[[#20]]ù´˜Ë‰[#012F ;Ê€<Y•ÑF§[[#4]]ç5}H€Ùje9â[[#7]]]ú¦œÕ´ Ü¶´è[[#5]][[#23]][[#11]]žF[[#8]]Ø¿[[#8]]	Block	1
77.91.153.121	Ukraine	147.237.72.166	aka.idf.il	Unknown Parameter amp;pagenum in www.aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
65.55.210.80	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at ¡[[#20]]ÜÁZ[[#15]]N¤-ˆVaFhˆg–[[#20]][[#19]]Ž,•Z7T§îf-ìÀ¾Ý°•F[[#2]]ìí»Rè‹ª„Žø£[[#3]]üÊ[[#1]]ü¬7[[#11]]Ø¦é%[[#5]]DúðU“?;^k•Ô2“,ú•6W8%[[#0]]cn2	Block	1
131.253.25.164	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-8517-he/atal.aspx	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
77.91.153.121	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-en/dover.aspx'	Block	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/3251.pdf	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Too Many Headers per Request - 28 Headers	Block	1
141.212.122.160	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1

03-12-2016-05:04:00 to 03-12-2016-06:04:00