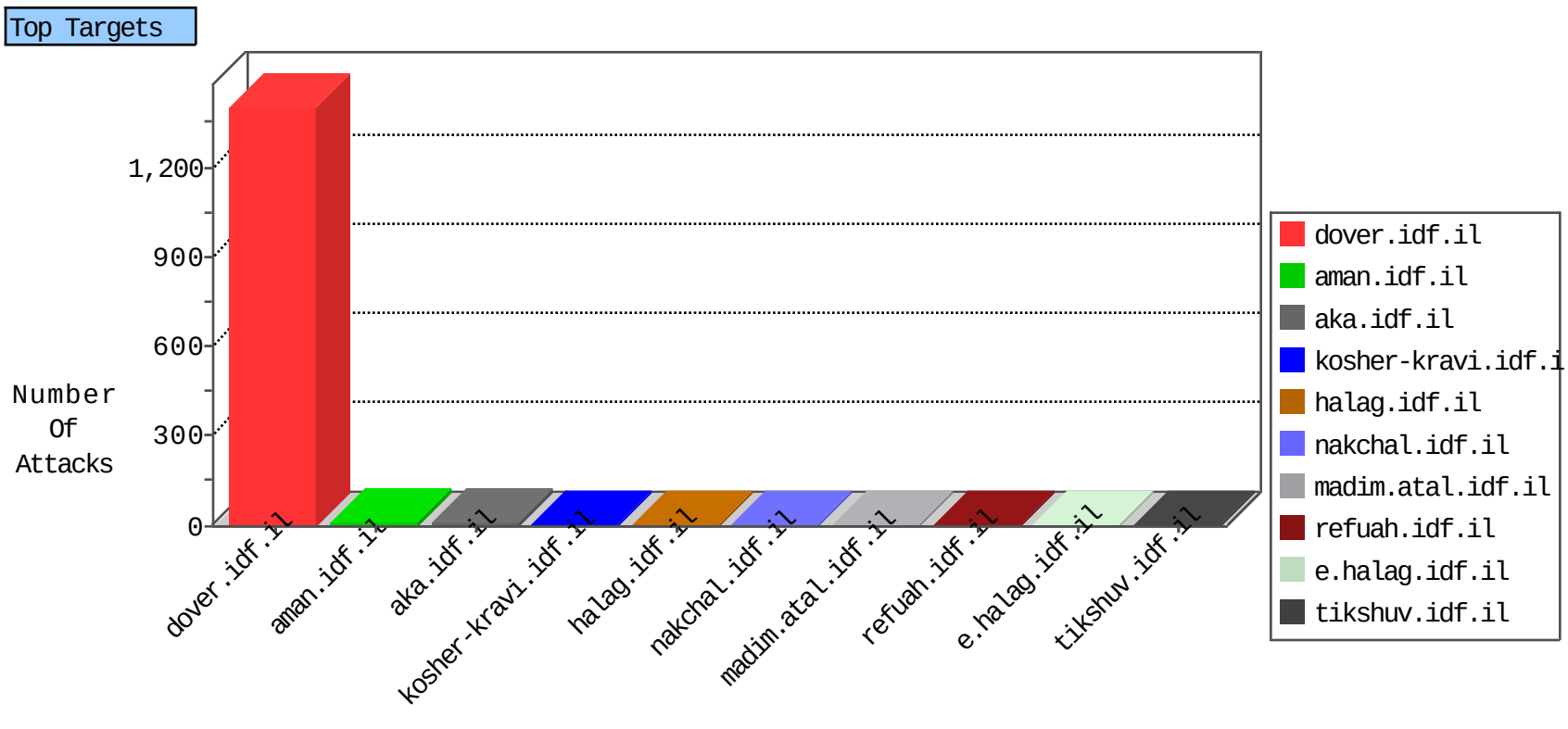
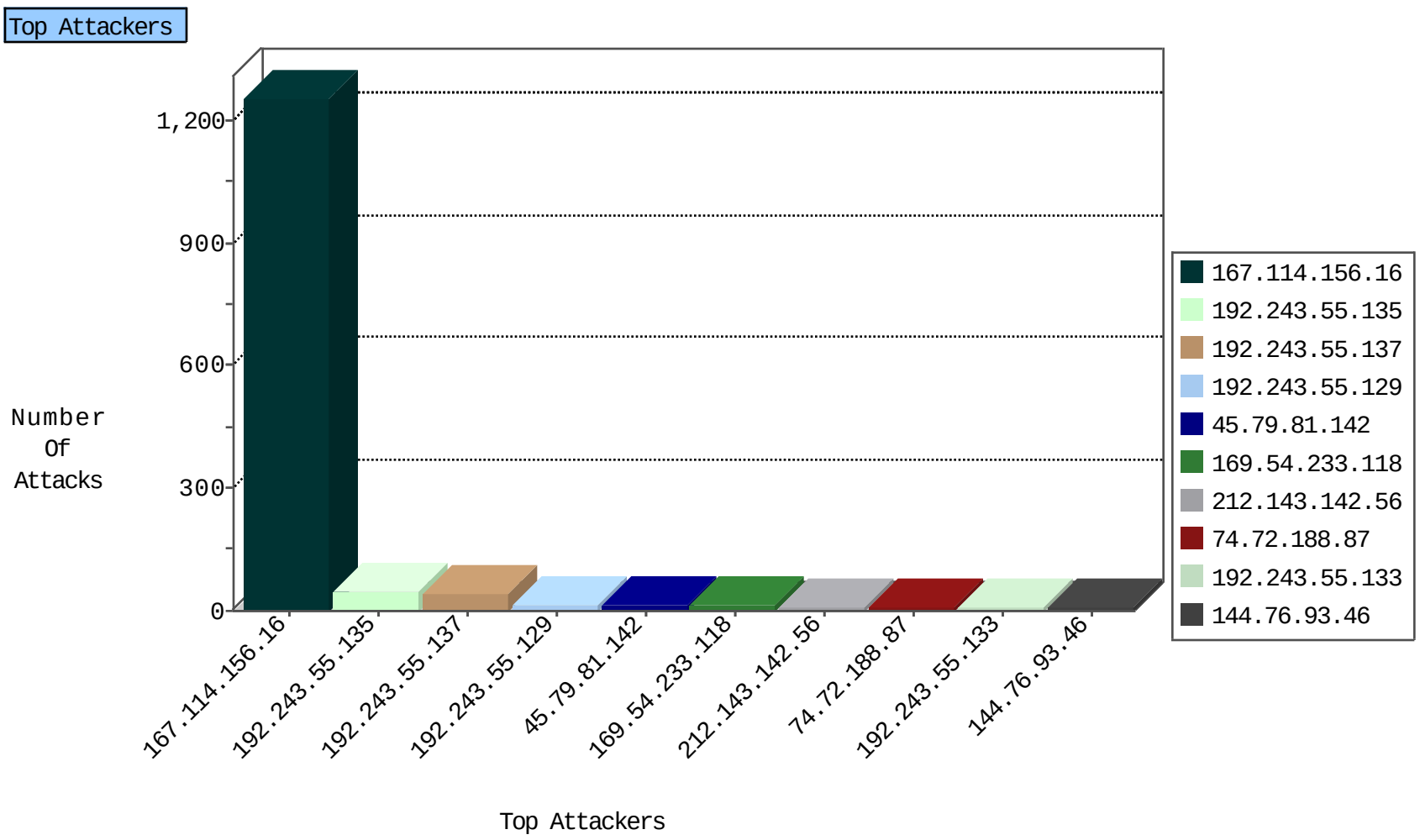
03-12-2016-06:04:03 to 03-12-2016-07:04:03

IDF Under Attack Daily Report





03-12-2016-06:04:03 to 03-12-2016-07:04:03

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	3996
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	2
184.105.139.112	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.33	Switzerland	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.96	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.206	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.116	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.72	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.96	United States	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.124	United States	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.72	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.108	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.80	United States	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1

03-12-2016-06:04:03 to 03-12-2016-07:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
144.76.93.46	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	4
144.76.93.46	Germany	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

03-12-2016-06:04:03 to 03-12-2016-07:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
169.54.233.118	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
169.54.233.118	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
184.80.10.136	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.118	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
169.54.233.118	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
169.54.233.118	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
169.54.233.118	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
169.54.233.118	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
169.54.233.118	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.79.243.160	147.237.77.216	Japan	dover.idf.il	Tehila - Perl LWP with fake user agent	1
59.45.79.117	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
184.80.10.136	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
184.80.10.136	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -f -sS	1
45.79.81.142	147.237.72.156		aman.idf.il	ET WEB_SERVER Poison Null Byte	1
169.54.233.118	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
169.54.233.118	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
169.54.233.118	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
169.54.233.118	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

03-12-2016-06:04:03 to 03-12-2016-07:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
74.72.188.87	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.231	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.172	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.52	United States	147.237.0.33	idf.il	drop		drop	1
184.105.139.86	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.161	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.72.188.87	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.240	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
157.55.39.134	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
81.218.84.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.91	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.162	United States	147.237.0.33	idf.il	drop		drop	1
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.12	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.247	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
89.247.35.98	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.99	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.163	United States	147.237.0.33	idf.il	drop		drop	1
74.82.47.15	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
174.118.251.160	Canada	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.207	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.171	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.30	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
216.218.206.79	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
74.72.188.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
46.19.85.184	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
199.30.24.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
87.71.50.246	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	2
87.71.50.246	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	2
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0113-3.stm`	Block	1
87.71.50.246	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/xmlrpc.php	Block	1
45.79.81.142		147.237.72.156	aman.idf.il	NULL Character in Method [[#22]][[#3]][[#1]][[#2]][[#0]][[#1]][[#0]][[#1]]ü[[#3]][[#3]]	Block	1
45.79.81.142		147.237.72.156	aman.idf.il	Abnormally Long Header Line request header name	Block	1
141.212.122.160	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/3250.jpg	Block	1
45.79.81.142		147.237.72.156	aman.idf.il	Illegal HTTP Version	Block	1
45.79.81.142		147.237.72.156	aman.idf.il	NULL Character in Parameter Name [[#19]][[#31]] FЋ/Þ[[#31]]˙ š[[#22]]Š[[#19]]/•'ÿ¥'ЊÊЋT$¡[[ƛ•#0[[]]#0,1, ,/,.,2,,0,p]] -[[#0]]£[[#0]]Ÿ[[#0]]¢[[#0]]ž,(,$,[[#20]], in Ý'ı×	Block	1
45.79.81.142		147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Name [[#0]]4[[#0]]2[[#0]][[#14]][[#0]]#012[[#0]][[#25]][[#0]][[#11]][[#0]][[#12]][[#0]][[#24]][[#0]]#011[[#0]]	Block	1
159.203.67.174	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unsupported Cipher	None	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/size100x0/2617.jpg	Block	1
45.79.81.142		147.237.72.156	aman.idf.il	Malformed HTTP Header Line 2	Block	1
199.30.25.157	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
45.79.81.142		147.237.72.156	aman.idf.il	NULL Character in Query String [[#19]][[#31]] FЋ/Þ[[#31]]˙ š[[#22]]Š[[#19]]/•'ÿ¥'ЊÊЋT$¡[[ƛ•#0[[]]#0,1, ,/,.,2,,0,p]] -[[#0]]£[[#0]]Ÿ[[#0]]¢[[#0]]ž,(,$,[[#20]], on Ý'ı×	Block	1
45.79.81.142		147.237.72.156	aman.idf.il	Illegal Byte Code Character in Method [[#22]][[#3]][[#1]][[#2]][[#0]][[#1]][[#0]][[#1]]ü[[#3]][[#3]]	Block	1
159.203.87.57	United States	147.237.76.39	mobile.meitav.idf.il	SSL Untraceable Connection - Unsupported Cipher	None	1
45.79.81.142		147.237.72.156	aman.idf.il	Malformed URL Ý'ı×	Block	1
110.55.0.49	Philippines	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
45.79.81.142		147.237.72.156	aman.idf.il	Unknown HTTP Request Method [[#22]][[#3]][[#1]][[#2]][[#0]][[#1]][[#0]][[#1]]ü[[#3]][[#3]] in URL Ý'ı×	Block	1
45.79.81.142		147.237.72.156	aman.idf.il	Illegal Byte Code Character in Parameter Name [[#19]][[#31]] FЋ/Þ[[#31]]˙ š[[#22]]Š[[#19]]/•'ÿ¥'ЊÊЋT$¡[[ƛ•#0[[]]#0,1, ,/,.,2,,0,p]] -[[#0]]£[[#0]]Ÿ[[#0]]¢[[#0]]ž,(,$,[[#20]], in Ý'ı×	Block	1
174.129.237.157	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
87.71.50.246	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
45.79.81.142		147.237.72.156	aman.idf.il	NULL Character in Header Name at [[#0]]ÿ[[#1]][[#0]][[#1]]c[[#0]][[#0]][[#0]][[#20]][[#0]][[#18]][[#0]][[#0]][[#15]]www.aman.idf.il[[#0]][[#11]][[#0]][[#4]][[#3]][[#0]][[#1]][[#2]][[#0]]	Block	1
40.77.167.82	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
110.55.0.49	Philippines	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
45.79.81.142		147.237.72.156	aman.idf.il	Illegal Byte Code Character in Query String [[#19]][[#31]] FЋ/Þ[[#31]]˙ š[[#22]]Š[[#19]]/•'ÿ¥'ЊÊЋT$¡[[ƛ•#0[[]]#0,1, ,/,.,2,,0,p]] -[[#0]]£[[#0]]Ÿ[[#0]]¢[[#0]]ž,(,$,[[#20]], on Ý'ı×	Block	1