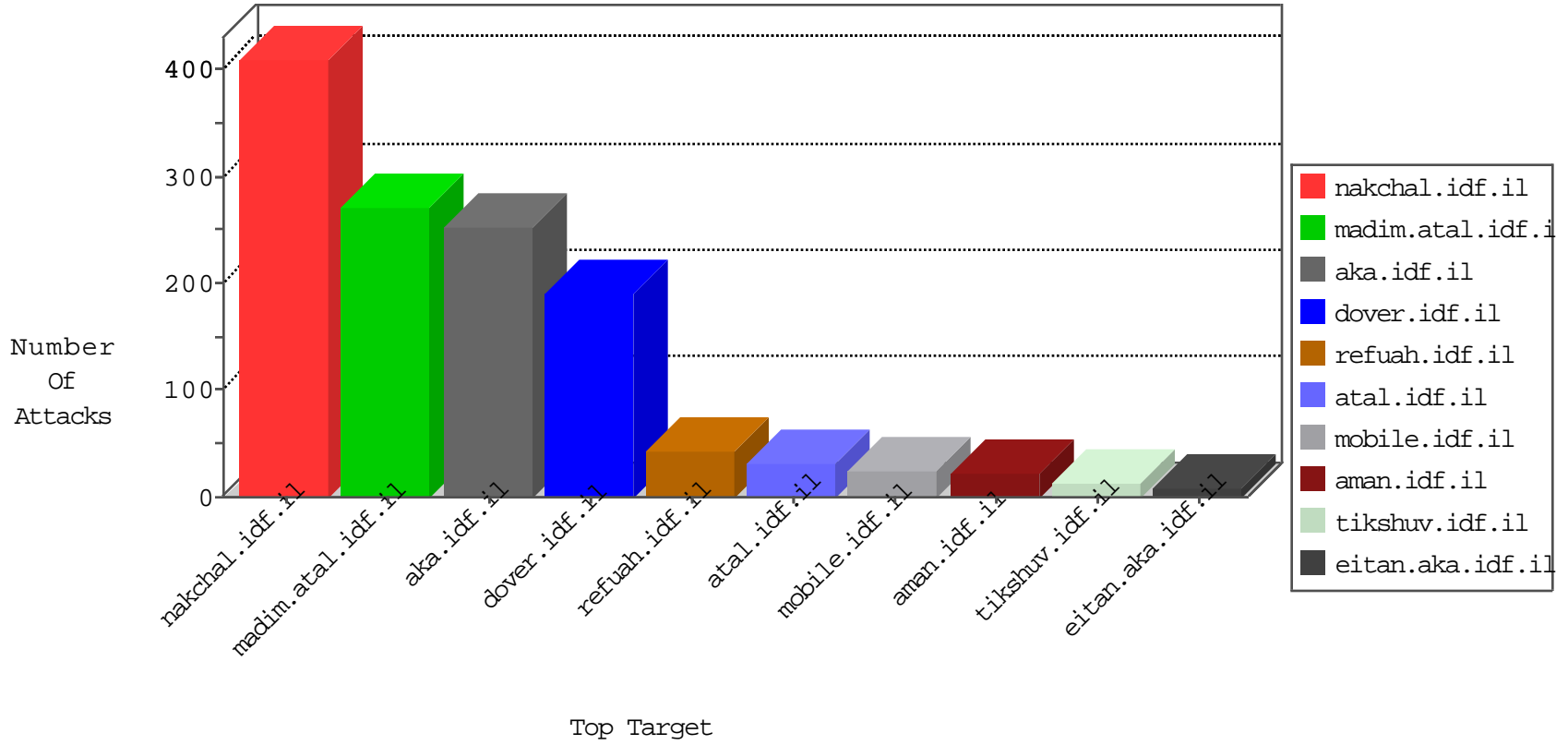


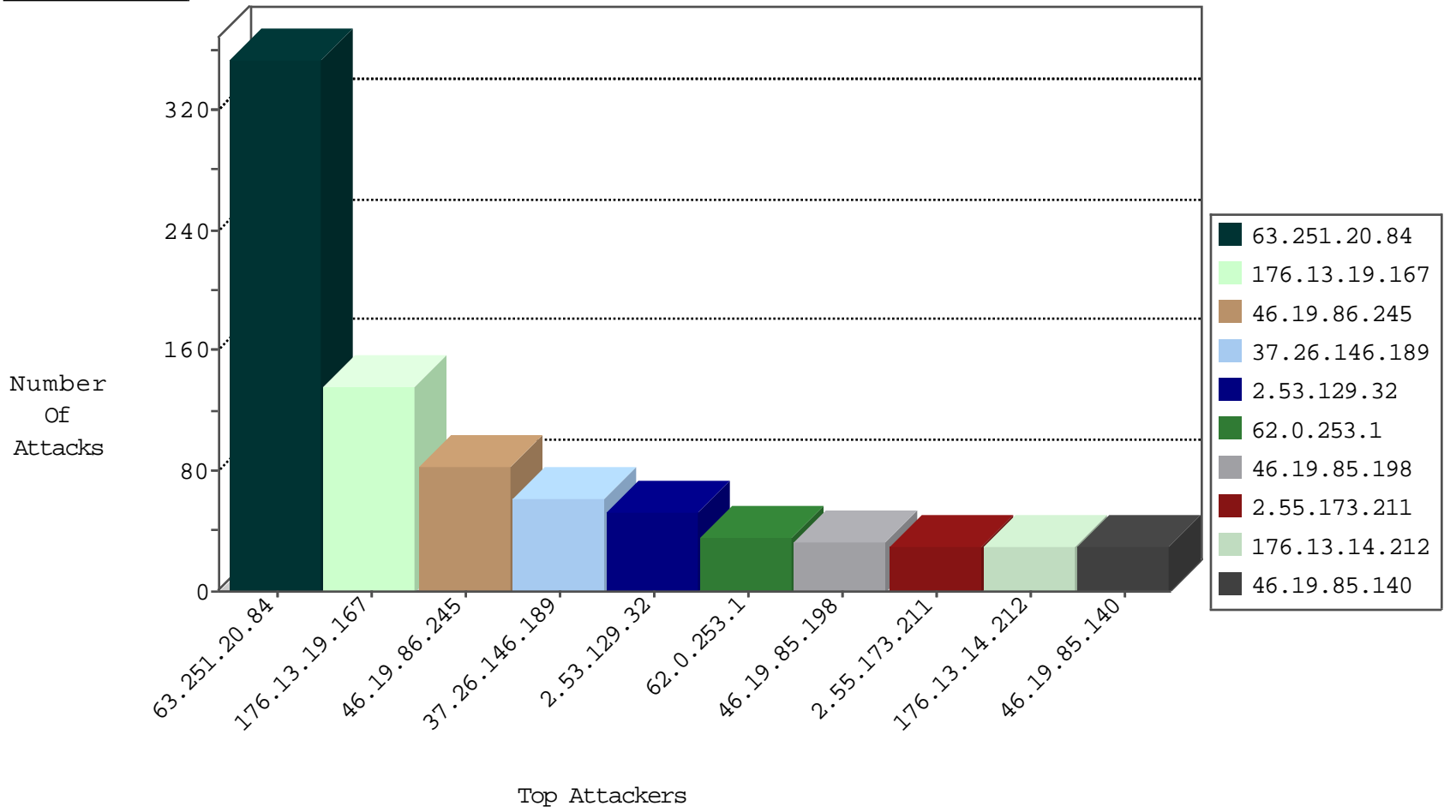
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.102.49.190	Netherlands	147.237.76.200	eitan.aka.idf.il	Black List	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.197.163.195	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.19.115.4	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	4
37.19.115.4	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
95.163.144.203	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
79.179.116.222	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.234.147	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
52.41.41.200	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.202.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.25.84.200	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.238.45	147.237.76.39	United Kingdom	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.77.176	United Kingdom	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.152.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.158.152	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.163.144.203	147.237.76.201	Russian Federation	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.49.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.220.2.5	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.28.189	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
212.76.112.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.234	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
207.232.50.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.158.177	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.136.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
63.251.20.84	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	342
62.0.253.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	36
46.19.85.140	Israel	147.237.77.233	atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
46.19.86.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
46.19.86.245	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
2.55.173.211	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
46.19.86.246	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	13
46.19.86.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.245	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
46.19.86.100	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
149.56.27.31	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
63.251.20.84	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
62.0.236.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
212.179.218.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
109.253.213.225	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
119.151.72.80	India	147.237.77.216	dover.idf.il	HTTP Format Sizes	'Proxy-Authorization' header length exceeded maximum allowed length	monitor	7
46.19.86.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.14.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.179.218.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
80.246.136.223	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.14.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
80.246.138.126	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.14.212	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	6
176.13.14.212	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
176.13.14.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.102.220.245	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.139.75.28	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
62.0.224.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.179.218.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
2.55.173.211	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
2.55.173.211	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
79.183.44.142	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
2.55.173.211	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
60.254.110.210	India	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
46.19.86.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.142.254.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
37.142.254.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
37.26.149.221	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
2.53.37.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
63.251.20.84	United States	147.237.76.31	nakchal.idf.il	SYN Attack		monitor	3
37.26.146.195	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.5.46	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.179	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.66	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
69.43.233.1	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.124.15.91	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.19.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	136
37.26.146.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
2.53.129.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
176.13.243.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
192.116.232.69	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	7
80.246.140.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
77.124.15.91	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	4
77.124.15.91	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 77.124.15.91	Block	3
46.19.86.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.140	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1437-he/atal.aspx	Block	2
37.26.146.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.110.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.55.6.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.138.126	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.79.18	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1
66.249.64.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct199 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
109.65.183.147	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	1
37.19.115.4	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	1
77.138.174.225	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
66.249.69.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9738-he/refuah.aspx	Block	1
2.55.17.91	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/23.03.04	Block	1
213.8.204.9	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
109.67.186.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
77.139.253.136	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.69.142	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8871-he/refuah.aspx	Block	1
46.19.85.140	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	1
193.105.199.1	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	1
82.80.156.82	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
213.8.204.9	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/xmlrpc.php	Block	1
66.249.64.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/60901.pdf	Block	1
2.53.12.211	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.178.220.41	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/recruitlane.aspx	Block	1
66.249.76.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1763	Block	1
193.105.199.1	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/3/	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.102.242.48	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
213.57.34.34	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
66.249.64.45	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/8/70008.doc	Block	1
37.26.149.206	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
80.246.136.223	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/70001.jpg	Block	1
46.19.86.245	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakchal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
194.90.200.70	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.200.70	Block	1
94.230.86.33	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.102.242.48	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 5.102.242.48	Block	1
77.124.15.91	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/4/	Block	1
66.249.69.81	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SearchText in www.eitan.aka.idf.il/938-en/eitan.aspx	None	1