Search Dashboard

Announcements Help

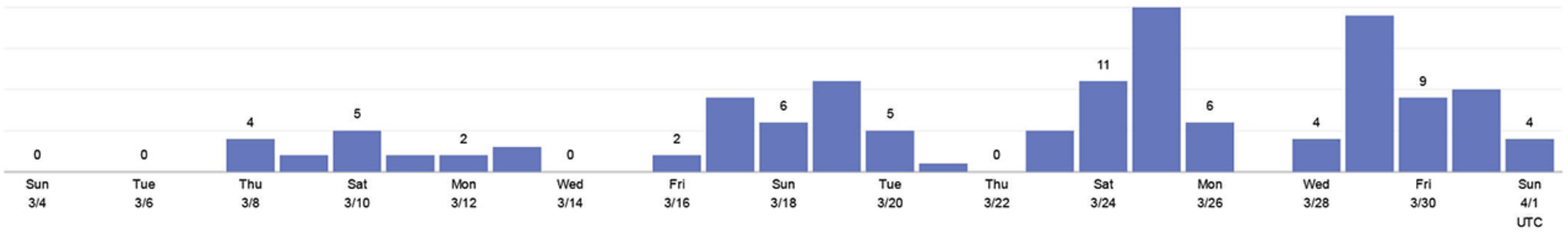
Security Center the last month

Search events

140 matching events All times are in UTC

Summary Events

Events over time



Most affected networks

Network	Events
CryptoWall	140

Most affected clients

Client	Network	Last Affected	Events
MacBook-Air Mac OS X 10.13	CryptoWall	Apr 1 2:43:10	83
DESKTOP Windows 10	CryptoWall	Mar 23 2:25:06	20
MacBook-Pro Mac OS X 10.13	CryptoWall	Apr 1 9:17:31	14
10-0-11-2 Android	CryptoWall	Mar 25 9:32:35	13
Android Android	CryptoWall	Mar 8 23:22:10	4
Android Android	CryptoWall	Mar 18 18:59:46	2
iPhone Apple iPhone	CryptoWall	Mar 21 23:29:30	2
MacBook-Pro Mac OS X 10.13	CryptoWall	Mar 11 18:23:58	1
MacBook-Pro Mac OS X 10.13	CryptoWall	Mar 29 9:57:30	1

Most prevalent threats

Threat	Occurrences
INDICATOR-COMPROMISE Suspicious .tk dns query	82
BROWSER-IE Microsoft Internet Explorer userdata behavior memory corruption attempt	27
INDICATOR-COMPROMISE Suspicious .win dns query	11
POLICY-OTHER CoinHive Miner client detected	4
BROWSER-PLUGINS Microsoft Internet Explorer MSXML .definition ActiveX clsid access attempt	3
POLICY-OTHER CoinHive Miner client detected	2
INDICATOR-COMPROMISE Suspicious .pw dns query	2
BROWSER-IE Microsoft Internet Explorer NodeFilter use after free attempt	2
INDICATOR-COMPROMISE .com- potentially malicious hostname	2
BROWSER-PLUGINS Microsoft Internet Explorer MSXML .definition ActiveX clsid access attempt	2

Most affected operating systems

OS	Events
Mac OS X 10.13	99
Windows 10	20
Android	19
Apple iPhone	2

Top sources of threats

IP	Country/Region	Events
104.27.241.251	United States	10
ec2-35-169-168-230.compute-1.amazonaws.com 35.169.168.230	United States	4
server-54-230-116-225.sfo9.r.cloudfront.net 54.230.116.225	United States	4
a23-45-229-204.deploy.static.akamaitechnologies.com 23.45.229.204	United States	4

IP	Country/Region	Events
server-54-192-140-144.sfo5.r.cloudfront.net 54.192.140.144	United States	3
104.27.240.251	United States	3
server-54-192-140-17.sfo5.r.cloudfront.net 54.192.140.17	United States	2
192.229.163.33	United States	2
ds10740.dreamservers.com 208.97.136.58	United States	2
server-54-230-144-122.sfo4.r.cloudfront.net 54.230.144.122	United States	1

Threats across networks

Threat Name	Networks
INDICATOR-COMPROMISE Suspicious .tk dns query	1
BROWSER-IE Microsoft Internet Explorer userdata behavior memory corruption attempt	1
INDICATOR-COMPROMISE Suspicious .win dns query	1
POLICY-OTHER CoinHive Miner client detected	1
BROWSER-PLUGINS Microsoft Internet Explorer MSXML .definition ActiveX clsid access attempt	1
POLICY-OTHER CoinHive Miner client detected	1
INDICATOR-COMPROMISE Suspicious .pw dns query	1