Analysis Report

ID	a426becd878212b98d78788d4e1682e9
OS	2600.xpsp_sp3_qfe.130704-0421
Started	5/23/17 17:20:45
Ended	5/23/17 17:28:56
Duration	0:08:11
Sandbox	mtv-work-093 (pilot-d)
Filename	Gartner Advice - Recognise and Respond to Today's Cybersecurity Threats.eml
Magic Type	RFC 822 mail, ASCII text, with very long lines, with CRLF line terminators
Analyzed As	mhtml
SHA256	`8b57e60ef843be3ad1f1ed145d9437e8eafe16d2bade030ed9040efcef9debc8`
SHA1	`2b3368e5678751324a49742571baaa0d96e158b6`
MD5	`d1473949d08da4bf063afbfc1381f73e`

Behavioral Indicators

Process Registered File as a File Handler	Severity: 100	Confidence: 85
Excessive Number of DNS Queries	Severity: 70	Confidence: 100
Javascript References Encryption/Decryption	Severity: 75	Confidence: 90
Javascript in HTML Uses Window.Open Function	Severity: 80	Confidence: 80
Javascript Contains an Excessively Long String	Severity: 80	Confidence: 80
Script Contains URL	Severity: 75	Confidence: 80
Outbound HTTP GET Request	Severity: 75	Confidence: 75
JavaScript Obfuscation Using "fromCharCode()" Function	Severity: 50	Confidence: 80
File Downloaded to Disk	Severity: 30	Confidence: 90
HTTP Redirection Response	Severity: 50	Confidence: 50

HTTP Client Error Response **Severity: 50** **Confidence: 50**

Remote IP Address Contacted **Severity: 20** **Confidence: 50**

URL Resulted in 404 or Empty File

HTTP Traffic

GET http://app.gartnerformarketers.com:80/e/er?utm_campaign=EVT_IN_2017_SECI3_E4_...87&elqat=1 Stream: 3 Transaction: 0

Server IP: 142.0.160.14 **Server Port**: 80 **Resp. Content**: text/html **Timestamp**: +215.0s

GET http://s1849907385.t.eloqua.com:80/e/er?utm_campaign=EVT_IN_2017_SECI3_E4_Glo...87&elqat=1 Stream: 5 Transaction: 0

Server IP: 142.0.160.13 **Server Port**: 80 **Resp. Content**: text/html **Timestamp**: +215.0s

GET http://s1849907385.t.eloqua.com:80/visitor/v200/svrGP?pps=3&siteid=1849907385...n=disabled Stream: 5 Transaction: 1

Server IP: 142.0.160.13 **Server Port**: 80 **Resp. Content**: image/gif **Timestamp**: +265.0s

GET http://s1849907385.t.eloqua.com:80/visitor/v200/svrGP?pps=3&siteid=1849907385...ity-india! Stream: 5 Transaction: 2

Server IP: 142.0.160.13 **Server Port**: 80 **Resp. Content**: image/gif **Timestamp**: +268.0s

GET http://s1849907385.t.eloqua.com:80/visitor/v200/svrGP?pps=3&siteid=1849907385...n=disabled Stream: 5 Transaction: 3

Server IP: 142.0.160.13 **Server Port**: 80 **Resp. Content**: image/gif **Timestamp**: +281.0s

GET http://app.gartnerformarketers.com:80/e/er?utm_campaign=EVT_IN_2017_SECI3_E4_...87&elqat=1 Stream: 6 Transaction: 0

Server IP: 142.0.160.14 **Server Port**: 80 **Resp. Content**: text/html **Timestamp**: +215.0s

GET http://s1849907385.t.eloqua.com:80/e/er?utm_campaign=EVT_IN_2017_SECI3_E4_Glo...87&elqat=1 Stream: 7 Transaction: 0

Server IP: 142.0.160.13 **Server Port**: 80 **Resp. Content**: text/html **Timestamp**: +215.0s

GET http://s1849907385.t.eloqua.com:80/visitor/v200/svrGP?pps=3&siteid=1849907385...n=disabled Stream: 7 Transaction: 1

Server IP: 142.0.160.13 **Server Port**: 80 **Resp. Content**: image/gif **Timestamp**: +230.0s

GET http://s1849907385.t.eloqua.com:80/visitor/v200/svrGP?pps=3&siteid=1849907385...ity-india! Stream: 7 Transaction: 2

Server IP: 142.0.160.13 **Server Port**: 80 **Resp. Content**: image/gif **Timestamp**: +231.0s

pps=3&siteid=1849907385...n=disabled

Server IP: 142.0.160.13 **Server Port**: 80 **Resp. Content**: image/gif **Timestamp**: +232.0s

---

GET http://www.gartner.com:80/events/apac/security-india?utm_campaign=EVT_IN_2017...kMA-_-0000 Stream: 9 Transaction: 0

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: text/html **Timestamp**: +216.0s

---

GET http://www.gartner.com:80/imagesrv/apps/gcms/events/css/stylesheets/main.min....7d4e52f58a Stream: 9 Transaction: 1

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +216.0s

---

GET http://www.gartner.com:80/imagesrv/apps/gcms/common/js/html5shiv-3.7.2.min.js...262af23e40 Stream: 9 Transaction: 2

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +217.0s

---

GET http://www.gartner.com:80/imagesrv/apps/gcms/events/css/stylesheets/bootstrap...gular.eot? Stream: 9 Transaction: 3

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: text/html **Timestamp**: +218.0s

---

GET http://www.gartner.com:80/events/apac/security-india?utm_campaign=EVT_IN_2017...kMA-_-0000 Stream: 10 Transaction: 0

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: text/html **Timestamp**: +216.0s

---

GET http://www.gartner.com:80/imagesrv/apps/gcms/events/css/stylesheets/main.min....7d4e52f58a Stream: 10 Transaction: 1

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +217.0s

---

GET http://www.gartner.com:80/imagesrv/apps/gcms/common/js/html5shiv-3.7.2.min.js...262af23e40 Stream: 10 Transaction: 2

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +218.0s

---

GET http://www.gartner.com:80/imagesrv/apps/gcms/events/js/gtmDataLayer.js;wa3c2b0a4c9e7825a4 Stream: 10 Transaction: 3

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/x-empty **Timestamp**: +219.0s

---

GET http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Fakt/FaktPro-Thin.eot? Stream: 10 Transaction: 4

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/x-empty **Timestamp**: +219.0s

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +220.0s

GET Stream: 10 Transaction: 6
http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Roboto/Robo...bfont.eot?

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +221.0s

GET http://www.gartner.com:80/imagesrv/apps/gcms/common/js/jquery-1.11.1.min.js;w...3f34f8b8be Stream: 11 Transaction: 0

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +217.0s

GET Stream: 11 Transaction: 1
http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Fakt/FaktPro-Bold.eot?

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +218.0s

GET Stream: 11 Transaction: 2
http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Fakt/FaktCo...edium.eot?

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +219.0s

GET Stream: 11 Transaction: 3
http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Roboto/Robo...bfont.eot?

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +219.0s

GET Stream: 11 Transaction: 4
http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/icons/Gartner.eot?

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +220.0s

GET Stream: 11 Transaction: 5
http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Roboto/Robo...bfont.eot?

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +220.0s

GET Stream: 11 Transaction: 6
http://www.gartner.com:80/imagesrv/apps/gcms/events/css/stylesheets/main.min....7d4e52f58a

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/x-empty **Timestamp**: +222.0s

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +225.0s

GET Stream: 11 Transaction: 8
http://www.gartner.com:80/imagesrv/apps/gcms/events/js/events.min.js;wa58ebf4f94787f212

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +225.0s

GET Stream: 11 Transaction: 9
http://www.gartner.com:80/binaries/content/gallery/events/standard/locations/mumbai.png

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +225.0s

GET http://cdn.optimizely.com:80/js/8025860307.js Stream: 13 Transaction: 0

Server IP: 23.0.246.17 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +217.0s

GET Stream: 14 Transaction: 0
http://www.gartner.com:80/imagesrv/apps/gcms/events/js/gtmDataLayer.js;wa3c2b0a4c9e7825a4

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +218.0s

GET Stream: 14 Transaction: 1
http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Fakt/FaktPro-Thin.eot?

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +218.0s

GET Stream: 14 Transaction: 2
http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Roboto/Robo...bfont.eot?

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +219.0s

GET http://oss.maxcdn.com:80/libs/respond.js/1.4.2/respond.min.js Stream: 16 Transaction: 0

Server IP: 146.88.138.90 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +218.0s

GET http://www.gartner.com:80/imagesrv/apps/gcms/common/js/jquery-1.11.1.min.js;w...3f34f8b8be Stream: 17 Transaction: 0

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +218.0s

GET Stream: 17 Transaction: 1
http://www.gartner.com:80/imagesrv/apps/gcms/events/css/stylesheets/bootstrap...gular.eot?

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: text/html **Timestamp**: +219.0s

GET http://cdn.optimizely.com:80/js/8025860307.js Stream: 18 Transaction: 0

Server IP: 23.0.246.17 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +219.0s

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +219.0s

GET http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Roboto/Robo...bfont.eot? Stream: 19 Transaction: 1

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +219.0s

GET http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Roboto/Robo...bfont.eot? Stream: 19 Transaction: 2

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +220.0s

GET http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Fakt/FaktPr...iBold.eot? Stream: 19 Transaction: 3

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +221.0s

GET http://www.gartner.com:80/imagesrv/apps/gcms/common/js/modernizr.custom.93545...8ff4ee9447 Stream: 19 Transaction: 4

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +225.0s

GET http://www.gartner.com:80/imagesrv/apps/gcms/common/js/bootstrap-3.2.0.min.js...36dacf519c Stream: 19 Transaction: 5

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +225.0s

GET http://www.gartner.com:80/imagesrv/apps/gcms/common/js/picturefill.min.js;wa2...23e6eb8dbd Stream: 19 Transaction: 6

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +225.0s

GET http://www.gartner.com:80/imagesrv/apps/gcms/common/js/jquery.flexslider-min....e475cfde4d Stream: 19 Transaction: 7

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +226.0s

GET http://www.gartner.com:80/imagesrv/apps/gcms/events/img/loading-grey.gif Stream: 19 Transaction: 8

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/gif **Timestamp**: +231.0s

GET Stream: 20 Transaction: 0
http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Fakt/FaktPr...talic.eot?

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms **Timestamp**: +219.0s

GET Stream: 20 Transaction: 1
http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Roboto/Robo...bfont.eot?

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +219.0s

---

GET Stream: 20 Transaction: 2
http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Roboto/Robo...bfont.eot?

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +220.0s

---

GET Stream: 20 Transaction: 3
http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Roboto/Robo...bfont.eot?

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +220.0s

---

GET http://www.gartner.com:80/binaries/content/gallery/events/standard/lead-gen/c...band_4.png Stream: 20 Transaction: 4

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +225.0s

---

GET http://www.gartner.com:80/favicon.ico Stream: 20 Transaction: 5

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/x-icon **Timestamp**: +226.0s

---

GET http://www.gartner.com:80/events/keywords/security/seci3/smarter-with-gartner?path= Stream: 20 Transaction: 6

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/javascript **Timestamp**: +231.0s

---

GET Stream: 21 Transaction: 0
http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Fakt/FaktPro-Bold.eot?

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/x-empty **Timestamp**: +219.0s

---

GET Stream: 21 Transaction: 1
http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Fakt/FaktPr...talic.eot?

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +219.0s

---

GET Stream: 21 Transaction: 2
http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Roboto/Robo...bfont.eot?

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +221.0s

Metadata | Behavioral Indicators | Network Activity | Processes | Artifacts | Registry Activity | File Activity

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +222.0s

GET Stream: 21 Transaction: 4
http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Roboto/Robo...bfont.eot?

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +223.0s

GET Stream: 21 Transaction: 5
http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Roboto/Robo...bfont.eot?

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +225.0s

GET http://www.gartner.com:80/binaries/content/gallery/events/standard/lead-gen/c...band_4.png Stream: 21 Transaction: 6

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +226.0s

GET http://www.gartner.com:80/favicon.ico Stream: 21 Transaction: 7

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/x-icon **Timestamp**: +228.0s

GET Stream: 22 Transaction: 0
http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Fakt/FaktPro-Blond.eot?

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +219.0s

GET Stream: 22 Transaction: 1
http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Roboto/Robo...bfont.eot?

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +221.0s

GET Stream: 22 Transaction: 2
http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/icons/Gartner.eot?

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +222.0s

GET Stream: 22 Transaction: 3
http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Roboto/Robo...bfont.eot?

Server IP: 206.16.239.65 **Server Port**: 80

Resp. Content: application/vnd.ms-fontobject **Timestamp**: +223.0s

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/x-empty **Timestamp**: +225.0s

GET http://www.gartner.com:80/imagesrv/apps/gcms/common/js/jquery.cookie.js;wa7234b21e99f75bcf Stream: 22 Transaction: 5

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/x-empty **Timestamp**: +226.0s

GET http://www.gartner.com:80/imagesrv/apps/gcms/common/js/jquery.flexslider-min....e475cfde4d Stream: 22 Transaction: 6

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/x-empty **Timestamp**: +226.0s

GET http://www.gartner.com:80/imagesrv/apps/gcms/events/js/events.min.js;wa58ebf4f94787f212 Stream: 22 Transaction: 7

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/x-empty **Timestamp**: +226.0s

GET http://www.gartner.com:80/imagesrv/apps/gcms/common/js/bootstrap-3.2.0.min.js...36dacf519c Stream: 22 Transaction: 8

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/x-empty **Timestamp**: +227.0s

GET http://www.gartner.com:80/imagesrv/apps/gcms/events/img/loading-grey.gif Stream: 22 Transaction: 9

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/x-empty **Timestamp**: +268.0s

GET http://www.gartner.com:80/events/keywords/security/seci3/smarter-with-gartner?path= Stream: 22 Transaction: 10

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/javascript **Timestamp**: +269.0s

GET http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Fakt/FaktPr...iBold.eot? Stream: 23 Transaction: 0

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +223.0s

GET http://www.gartner.com:80/imagesrv/apps/gcms/common/fonts/gartner/Roboto/Robo...bfont.eot? Stream: 23 Transaction: 1

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/vnd.ms-fontobject **Timestamp**: +225.0s

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/x-empty **Timestamp**: +226.0s

GET Stream: 23 Transaction: 3
http://www.gartner.com:80/imagesrv/apps/gcms/common/js/picturefill.min.js;wa2...23e6eb8dbd

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/x-empty **Timestamp**: +226.0s

GET Stream: 23 Transaction: 4
http://www.gartner.com:80/binaries/content/gallery/events/standard/locations/mumbai.png

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +226.0s

GET Stream: 30 Transaction: 0
http://na2.www.gartner.com:80/binaries/content/gallery/events/standard/event-...398a5538d1

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +224.0s

GET Stream: 30 Transaction: 1
http://na2.www.gartner.com:80/binaries/content/gallery/events/standard/speake...da7f404c6c

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +225.0s

GET Stream: 32 Transaction: 0
http://na3.www.gartner.com:80/binaries/content/gallery/events/standard/hero/s...e00b45c795

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +224.0s

GET Stream: 32 Transaction: 1
http://na3.www.gartner.com:80/binaries/content/gallery/events/standard/speake...3ec35431f3

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +225.0s

GET Stream: 32 Transaction: 2
http://na3.www.gartner.com:80/imagesrv/apps/gcms/events/img/gartner.png;wabfaaf6d795a18c1e

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +225.0s

GET Stream: 33 Transaction: 0
http://na3.www.gartner.com:80/binaries/content/gallery/events/standard/hero/g...2172df1183

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +224.0s

GET Stream: 33 Transaction: 1
http://na3.www.gartner.com:80/binaries/content/gallery/events/standard/speake...4152ec1525

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +225.0s

GET Stream: 35 Transaction: 0

GET http://na1.www.gartner.com:80/imagesrv/apps/gcms/events/img/loading-grey.gif;...f35fed0078 Stream: 35 Transaction: 1

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/gif **Timestamp**: +225.0s

GET Stream: 36 Transaction: 0
http://na2.www.gartner.com:80/binaries/content/gallery/events/standard/hero/s...38af55fc13

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +224.0s

GET Stream: 36 Transaction: 1
http://na2.www.gartner.com:80/binaries/content/gallery/events/standard/speake...5d5a462be0

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +225.0s

GET Stream: 38 Transaction: 0
http://cdnapi.kaltura.com:80/p/585951/sp/58595100/embedIframeJs/uiconf_id/318..._id/585951

Server IP: 165.254.47.106 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +224.0s

GET Stream: 38 Transaction: 1
http://cdnapi.kaltura.com:80/p/585951/sp/58595100/embedIframeJs/uiconf_id/318...5574664484

Server IP: 165.254.47.106 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +232.0s

GET Stream: 42 Transaction: 0
http://na2.www.gartner.com:80/binaries/content/gallery/events/standard/event-...398a5538d1

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +225.0s

GET Stream: 42 Transaction: 1
http://na2.www.gartner.com:80/binaries/content/gallery/events/standard/speake...da7f404c6c

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +226.0s

GET Stream: 43 Transaction: 0
http://na3.www.gartner.com:80/binaries/content/gallery/events/standard/hero/s...e00b45c795

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +225.0s

GET Stream: 43 Transaction: 1
http://na3.www.gartner.com:80/binaries/content/gallery/events/standard/speake...3ec35431f3

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +226.0s

GET Stream: 43 Transaction: 2
http://na3.www.gartner.com:80/imagesrv/apps/gcms/events/img/gartner.png;wabfaaf6d795a18c1e

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/x- **Timestamp**: +226.0s

GET Stream: 44 Transaction: 0
http://na1.www.gartner.com:80/binaries/content/gallery/events/standard/hero/s...751091f084

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +225.0s

GET Stream: 45 Transaction: 0
http://na2.www.gartner.com:80/binaries/content/gallery/events/standard/hero/s...38af55fc13

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +225.0s

GET Stream: 45 Transaction: 1
http://na2.www.gartner.com:80/binaries/content/gallery/events/standard/speake...5d5a462be0

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +226.0s

GET Stream: 46 Transaction: 0
http://na3.www.gartner.com:80/binaries/content/gallery/events/standard/hero/g...2172df1183

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +225.0s

GET Stream: 46 Transaction: 1
http://na3.www.gartner.com:80/binaries/content/gallery/events/standard/speake...4152ec1525

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +226.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=event...-46045.jpg Stream: 48 Transaction: 0

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +225.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=event...-45403.png Stream: 48 Transaction: 1

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +225.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=event...-45399.png Stream: 49 Transaction: 0

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +225.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=event...-45400.png Stream: 49 Transaction: 1

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +225.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=event...-45397.png Stream: 50 Transaction: 0

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +225.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx? Stream: 50 Transaction: 1

Metadata | Behavioral Indicators | Network Activity | Processes | Artifacts | Registry Activity | File Activity

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=event...-45402.jpg Stream: 51 Transaction: 0

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +225.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=event...-45404.png Stream: 51 Transaction: 1

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +225.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=event...-46044.png Stream: 52 Transaction: 0

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +225.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=event...-45406.png Stream: 52 Transaction: 1

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +225.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=event...-45405.png Stream: 53 Transaction: 0

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +225.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=globa...n-1915.jpg Stream: 53 Transaction: 1

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +225.0s

GET http://na1.www.gartner.com:80/imagesrv/apps/gcms/events/img/loading-grey.gif;...f35fed0078 Stream: 54 Transaction: 0

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: application/x-empty **Timestamp**: +225.0s

GET http://na1.www.gartner.com:80/binaries/content/gallery/events/keywords/securi...61a1b7eb71 Stream: 54 Transaction: 1

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +278.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=event...-45401.jpg Stream: 55 Transaction: 0

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +226.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=event...-45406.png Stream: 55 Transaction: 1

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +226.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=event...-45399.png Stream: 55 Transaction: 2

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +226.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=event...-45400.png Stream: 55 Transaction: 3

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +227.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=event...-45403.png Stream: 56 Transaction: 0

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +226.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=event...-46045.jpg Stream: 56 Transaction: 1

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +226.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=event...-45405.png Stream: 56 Transaction: 2

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +226.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=event...-45402.jpg Stream: 56 Transaction: 3

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +227.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=event...-45397.png Stream: 57 Transaction: 0

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +226.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=event...-46044.png Stream: 57 Transaction: 1

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +226.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=event...-45404.png Stream: 57 Transaction: 2

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/png **Timestamp**: +227.0s

GET http://agendabuilder.gartner.com:80/handlers/imagehandler.ashx?location=globa...n-1915.jpg Stream: 57 Transaction: 3

Server IP: 207.140.148.117 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +227.0s

GET http://img.en25.com:80/i/elqCfg.min.js Stream: 59 Transaction: 0

GET http://a.adroll.com:80/j/roundtrip.js

Server IP: 165.254.47.113 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +230.0s

GET http://static.hotjar.com:80/c/hotjar-64884.js?sv=5 Stream: 67 Transaction: 0

Server IP: 198.232.124.194 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +230.0s

GET http://js.bizographics.com:80/insight.min.js Stream: 71 Transaction: 0

Server IP: 54.192.118.64 **Server Port**: 80 **Resp. Content**: application/x-empty **Timestamp**: +230.0s

GET http://cdn.justuno.com:80/coupon_code1.js Stream: 72 Transaction: 0

Server IP: 185.180.13.16 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +230.0s

GET http://cdn.justuno.com:80/mwgt_3.6.js Stream: 72 Transaction: 1

Server IP: 185.180.13.16 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +230.0s

GET http://dnn506yrbagrg.cloudfront.net:80/pages/scripts/0056/3437.js?415437 Stream: 75 Transaction: 0

Server IP: 54.192.117.84 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +230.0s

GET http://www.justuno.com:80/ajax/account_version_check.html?id=315C73F4-A28C-41...1C5B018960 Stream: 80 Transaction: 0

Server IP: 50.56.156.22 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +230.0s

GET http://na1.www.gartner.com:80/binaries/content/gallery/events/keywords/securi...5f03cc1390 Stream: 102 Transaction: 0

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +232.0s

GET http://na1.www.gartner.com:80/binaries/content/gallery/events/keywords/securi...61a1b7eb71 Stream: 103 Transaction: 0

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +232.0s

GET http://na3.www.gartner.com:80/binaries/content/gallery/events/keywords/securi...9be2fb69a8 Stream: 104 Transaction: 0

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +232.0s

GET http://na2.www.gartner.com:80/binaries/content/gallery/events/keywords/securi...75c029782c Stream: 105 Transaction: 0

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +232.0s

GET Stream: 105 Transaction: 1
http://na2.www.gartner.com:80/binaries/content/gallery/events/keywords/securi...64bb08c937

http://na2.www.gartner.com:80/binaries/content/gallery/events/keywords/securi...b93418358d

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +232.0s

GET http://img.en25.com:80/i/elqCfg.min.js Stream: 113 Transaction: 0

Server IP: 23.32.91.103 **Server Port**: 80 **Resp. Content**: application/x-empty **Timestamp**: +265.0s

GET http://js.bizographics.com:80/insight.min.js Stream: 116 Transaction: 0

Server IP: 54.192.118.64 **Server Port**: 80 **Resp. Content**: application/x-empty **Timestamp**: +267.0s

GET Stream: 121 Transaction: 0
http://na1.www.gartner.com:80/binaries/content/gallery/events/keywords/securi...5f03cc1390

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +279.0s

GET Stream: 122 Transaction: 0
http://na3.www.gartner.com:80/binaries/content/gallery/events/keywords/securi...9be2fb69a8

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +279.0s

GET Stream: 123 Transaction: 0
http://na2.www.gartner.com:80/binaries/content/gallery/events/keywords/securi...64bb08c937

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +279.0s

GET Stream: 123 Transaction: 1
http://na2.www.gartner.com:80/binaries/content/gallery/events/keywords/securi...75c029782c

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +281.0s

GET Stream: 124 Transaction: 0
http://na2.www.gartner.com:80/binaries/content/gallery/events/keywords/securi...b93418358d

Server IP: 206.16.239.65 **Server Port**: 80 **Resp. Content**: image/jpeg **Timestamp**: +279.0s

GET Stream: 126 Transaction: 0
http://cdnapi.kaltura.com:80/p/585951/sp/58595100/embedIframeJs/uiconf_id/318...5574665125

Server IP: 165.254.47.107 **Server Port**: 80 **Resp. Content**: text/plain **Timestamp**: +282.0s

DNS Traffic

TTL: - **Timestamp**: +215.165s

Query Type: A, Query Data: s1849907385.t.eloqua.com Stream: 4 Query: 46324
TTL: - **Timestamp**: +215.424s

Query Type: A, Query Data: www.gartner.com Stream: 8 Query: 35212
TTL: - **Timestamp**: +216.121s

Query Type: A, Query Data: cdn.optimizely.com Stream: 12 Query: 38437
TTL: - **Timestamp**: +216.783s

Query Type: A, Query Data: oss.maxcdn.com Stream: 15 Query: 10129
TTL: - **Timestamp**: +218.146s

Query Type: A, Query Data: www.googletagmanager.com Stream: 24 Query: 9296
TTL: - **Timestamp**: +223.113s

Query Type: A, Query Data: platform.twitter.com Stream: 25 Query: 45130
TTL: - **Timestamp**: +223.141s

Query Type: A, Query Data: na2.www.gartner.com Stream: 29 Query: 55698
TTL: - **Timestamp**: +223.877s

Query Type: A, Query Data: na3.www.gartner.com Stream: 31 Query: 629
TTL: - **Timestamp**: +224.365s

Query Type: A, Query Data: na1.www.gartner.com Stream: 34 Query: 6432
TTL: - **Timestamp**: +224.535s

Query Type: A, Query Data: cdnapi.kaltura.com Stream: 37 Query: 31782
TTL: - **Timestamp**: +224.765s

Query Type: A, Query Data: agendabuilder.gartner.com Stream: 47 Query: 36575
TTL: - **Timestamp**: +225.534s

Query Type: A, Query Data: img.en25.com Stream: 58 Query: 45702
TTL: - **Timestamp**: +230.127s

Query Type: A, Query Data: a.adroll.com Stream: 60 Query: 47087
TTL: - **Timestamp**: +230.265s

Query Type: A, Query Data: www.google-analytics.com Stream: 62 Query: 61661
TTL: - **Timestamp**: +230.286s

Query Type: A, Query Data: dnn506yrbagrg.cloudfront.net Stream: 64 Query: 54144

TTL: - **Timestamp**: +230.315s

Query Type: A, Query Data: static.hotjar.com Stream: 65 Query: 639

TTL: - **Timestamp**: +230.321s

TTL: - **Timestamp**: +230.325s

Query Type: A, Query Data: connect.facebook.net Stream: 68 Query: 7727

TTL: - **Timestamp**: +230.34s

Query Type: A, Query Data: cdn.justuno.com Stream: 70 Query: 55253

TTL: - **Timestamp**: +230.378s

Query Type: A, Query Data: snap.licdn.com Stream: 73 Query: 30471

TTL: - **Timestamp**: +230.4s

Query Type: A, Query Data: d.adroll.com Stream: 76 Query: 55355

TTL: - **Timestamp**: +230.487s

Query Type: A, Query Data: www.justuno.com Stream: 79 Query: 11358

TTL: - **Timestamp**: +230.807s

Query Type: A, Query Data: dc.ads.linkedin.com Stream: 81 Query: 2484

TTL: - **Timestamp**: +230.812s

Query Type: A, Query Data: stats.g.doubleclick.net Stream: 83 Query: 23606

TTL: - **Timestamp**: +230.83s

Query Type: A, Query Data: www.bizographics.com Stream: 86 Query: 44334

TTL: - **Timestamp**: +230.994s

Query Type: A, Query Data: www.google.com Stream: 88 Query: 15787

TTL: - **Timestamp**: +231.01s

Query Type: A, Query Data: us-west-2.dc.ads.linkedin.com Stream: 91 Query: 9745

TTL: - **Timestamp**: +231.21s

Query Type: A, Query Data: secure.adnxs.com Stream: 93 Query: 21050

TTL: - **Timestamp**: +231.354s

Query Type: A, Query Data: www.linkedin.com Stream: 95 Query: 14173

TTL: - **Timestamp**: +231.544s

Query Type: A, Query Data: gtrk.s3.amazonaws.com Stream: 97 Query: 1537

TTL: - **Timestamp**: +232.197s

Query Type: A, Query Data: cm.g.doubleclick.net Stream: 100 Query: 45449

TTL: - **Timestamp**: +232.249s

Query Type: A, Query Data: imp2.ads.linkedin.com Stream: 107 Query: 28801

TTL: - **Timestamp**: +232.332s

Query Type: A, Query Data: img.en25.com Stream: 112 Query: 17491
TTL: - **Timestamp**: +265.096s

Query Type: A, Query Data: odnoklassniki-kultura.com Stream: 125 Query: 20860

Query Type: A, Query Data: imp2.ads.linkedin.com Stream: 128 Query: 60680
TTL: - **Timestamp**: +285.331s

TCP/IP Streams

Network Stream: 0
Src. IP 0.0.0.0 **Src. Port** 68 **Dest. IP** 255.255.255.255 **Dest. Port** 67 **Transport** UDP
Artifacts 0 **Packets** 2 **Bytes** 661 **Timestamp** +36.018s

Network Stream: 1 (DHCP)
Src. IP 192.168.1.148 **Src. Port** 68 **Dest. IP** 192.168.1.1 **Dest. Port** 67 **Transport** UDP
Artifacts 0 **Packets** 2 **Bytes** 664 **Timestamp** +36.018s

Network Stream: 2 (DNS)
Src. IP 192.168.1.148 **Src. Port** 55563 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
Artifacts 0 **Packets** 2 **Bytes** 213 **Timestamp** +215.165s

Network Stream: 3 (HTTP)
Src. IP 192.168.1.148 **Src. Port** 1094 **Dest. IP** 142.0.160.14 **Dest. Port** 80 **Transport** TCP
Artifacts 0 **Packets** 8 **Bytes** 2029 **Timestamp** +215.17s

Network Stream: 4 (DNS)
Src. IP 192.168.1.148 **Src. Port** 60856 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
Artifacts 0 **Packets** 2 **Bytes** 174 **Timestamp** +215.424s

Network Stream: 5 (HTTP)
Src. IP 192.168.1.148 **Src. Port** 1095 **Dest. IP** 142.0.160.13 **Dest. Port** 80 **Transport** TCP
Artifacts 0 **Packets** 20 **Bytes** 5681 **Timestamp** +215.426s

Network Stream: 6 (HTTP)
Src. IP 192.168.1.148 **Src. Port** 1097 **Dest. IP** 142.0.160.14 **Dest. Port** 80 **Transport** TCP
Artifacts 1 **Packets** 8 **Bytes** 2029 **Timestamp** +215.584s

Network Stream: 7 (HTTP)

Src. **Src. Port** 1098 **Dest. IP** 142.0.160.13 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 2 **Packets** 20 **Bytes** 5463 **Timestamp** +215.903s

IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 138 **Timestamp** +216.121s

Network Stream: 9 (HTTP)
Src. **Src. Port** 1099 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 4 **Packets** 131 **Bytes** 99439 **Timestamp** +216.167s

Network Stream: 10 (HTTP)
Src. **Src. Port** 1100 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 1 **Packets** 283 **Bytes** 228804 **Timestamp** +216.218s

Network Stream: 11 (HTTP)
Src. **Src. Port** 1101 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 8 **Packets** 1215 **Bytes** 1096239 **Timestamp** +216.707s

Network Stream: 12 (DNS)
Src. **Src. Port** 55911 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 144 **Timestamp** +216.783s

Network Stream: 13 (HTTP)
Src. **Src. Port** 1102 **Dest. IP** 23.0.246.17 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 0 **Packets** 40 **Bytes** 43396 **Timestamp** +216.84s

Network Stream: 14 (HTTP)
Src. **Src. Port** 1103 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 2 **Packets** 185 **Bytes** 134469 **Timestamp** +217.82s

Network Stream: 15 (DNS)
Src. **Src. Port** 57665 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 178 **Timestamp** +218.146s

Network Stream: 16 (HTTP)
Src. **Src. Port** 1105 **Dest. IP** 146.88.138.90 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 1 **Packets** 11 **Bytes** 3743 **Timestamp** +218.151s

Network Stream: 17 (HTTP)

Src. IP 192.168.1.148 **Src. Port** 1104 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP

Network Stream: 18 (HTTP)

Src. IP 192.168.1.148 **Src. Port** 1106 **Dest. IP** 23.0.246.17 **Dest. Port** 80 **Transport** TCP

Artifacts 1 **Packets** 41 **Bytes** 43517 **Timestamp** +218.658s

Network Stream: 19 (HTTP)

Src. IP 192.168.1.148 **Src. Port** 1107 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP

Artifacts 7 **Packets** 385 **Bytes** 337468 **Timestamp** +218.66s

Network Stream: 20 (HTTP)

Src. IP 192.168.1.148 **Src. Port** 1108 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP

Artifacts 2 **Packets** 658 **Bytes** 593885 **Timestamp** +218.688s

Network Stream: 21 (HTTP)

Src. IP 192.168.1.148 **Src. Port** 1109 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP

Artifacts 5 **Packets** 682 **Bytes** 615535 **Timestamp** +219.322s

Network Stream: 22 (HTTP)

Src. IP 192.168.1.148 **Src. Port** 1110 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP

Artifacts 3 **Packets** 288 **Bytes** 221411 **Timestamp** +219.619s

Network Stream: 23 (HTTP)

Src. IP 192.168.1.148 **Src. Port** 1111 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP

Artifacts 1 **Packets** 908 **Bytes** 842497 **Timestamp** +222.844s

Network Stream: 24 (DNS)

Src. IP 192.168.1.148 **Src. Port** 51154 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP

Artifacts 0 **Packets** 2 **Bytes** 200 **Timestamp** +223.113s

Network Stream: 25 (DNS)

Src. IP 192.168.1.148 **Src. Port** 58357 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP

Artifacts 0 **Packets** 2 **Bytes** 308 **Timestamp** +223.141s

Network Stream: 26

Src. IP 192.168.1.148 **Src. Port** 1112 **Dest. IP** 216.58.219.40 **Dest. Port** 443 **Transport** TCP

Artifacts 3 **Packets** 60 **Bytes** 50757 **Timestamp** +223.154s

Network Stream: 27

Src. **Src. Port** 1113 **Dest. IP** 192.229.163.25 **Dest. Port** 443 **Transport** TCP

Network Stream: 28

Src. **Src. Port** 1114 **Dest. IP** 192.229.163.25 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 0 **Packets** 6 **Bytes** 337 **Timestamp** +223.33s

Network Stream: 29 (DNS)

Src. **Src. Port** 49276 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 160 **Timestamp** +223.877s

Network Stream: 30 (HTTP)

Src. **Src. Port** 1115 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 0 **Packets** 159 **Bytes** 108235 **Timestamp** +223.967s

Network Stream: 31 (DNS)

Src. **Src. Port** 61283 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 160 **Timestamp** +224.365s

Network Stream: 32 (HTTP)

Src. **Src. Port** 1116 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 1 **Packets** 333 **Bytes** 249609 **Timestamp** +224.461s

Network Stream: 33 (HTTP)

Src. **Src. Port** 1117 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 1 **Packets** 492 **Bytes** 431427 **Timestamp** +224.517s

Network Stream: 34 (DNS)

Src. **Src. Port** 53938 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 160 **Timestamp** +224.535s

Network Stream: 35 (HTTP)

Src. **Src. Port** 1118 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 2 **Packets** 149 **Bytes** 97419 **Timestamp** +224.592s

Network Stream: 36 (HTTP)

Src. **Src. Port** 1119 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 0 **Packets** 367 **Bytes** 273200 **Timestamp** +224.66s

IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 235 **Timestamp** +224.765s

Network Stream: 38 (HTTP)
Src. **Src. Port** 1120 **Dest. IP** 165.254.47.106 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 1 **Packets** 54 **Bytes** 47014 **Timestamp** +224.815s

Network Stream: 39
Src. **Src. Port** 1121 **Dest. IP** 216.58.219.40 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 3 **Packets** 62 **Bytes** 50693 **Timestamp** +225.406s

Network Stream: 40
Src. **Src. Port** 1122 **Dest. IP** 192.229.163.25 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 0 **Packets** 10 **Bytes** 504 **Timestamp** +225.416s

Network Stream: 41
Src. **Src. Port** 1123 **Dest. IP** 192.229.163.25 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 0 **Packets** 6 **Bytes** 337 **Timestamp** +225.442s

Network Stream: 42 (HTTP)
Src. **Src. Port** 1124 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 2 **Packets** 138 **Bytes** 107553 **Timestamp** +225.445s

Network Stream: 43 (HTTP)
Src. **Src. Port** 1125 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 2 **Packets** 311 **Bytes** 246251 **Timestamp** +225.45s

Network Stream: 44 (HTTP)
Src. **Src. Port** 1126 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 0 **Packets** 134 **Bytes** 68216 **Timestamp** +225.451s

Network Stream: 45 (HTTP)
Src. **Src. Port** 1127 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 2 **Packets** 343 **Bytes** 272367 **Timestamp** +225.452s

Network Stream: 46 (HTTP)

Src. IP 192.168.1.148 **Src. Port** 1128 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP

Network Stream: 47 (DNS)

Src. IP 192.168.1.148 **Src. Port** 50138 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP

Artifacts 0 **Packets** 2 **Bytes** 158 **Timestamp** +225.534s

Network Stream: 48 (HTTP)

Src. IP 192.168.1.148 **Src. Port** 1129 **Dest. IP** 207.140.148.117 **Dest. Port** 80 **Transport** TCP

Artifacts 0 **Packets** 19 **Bytes** 10807 **Timestamp** +225.588s

Network Stream: 49 (HTTP)

Src. IP 192.168.1.148 **Src. Port** 1130 **Dest. IP** 207.140.148.117 **Dest. Port** 80 **Transport** TCP

Artifacts 1 **Packets** 26 **Bytes** 18662 **Timestamp** +225.588s

Network Stream: 50 (HTTP)

Src. IP 192.168.1.148 **Src. Port** 1131 **Dest. IP** 207.140.148.117 **Dest. Port** 80 **Transport** TCP

Artifacts 1 **Packets** 23 **Bytes** 15386 **Timestamp** +225.589s

Network Stream: 51 (HTTP)

Src. IP 192.168.1.148 **Src. Port** 1132 **Dest. IP** 207.140.148.117 **Dest. Port** 80 **Transport** TCP

Artifacts 2 **Packets** 21 **Bytes** 12146 **Timestamp** +225.589s

Network Stream: 52 (HTTP)

Src. IP 192.168.1.148 **Src. Port** 1133 **Dest. IP** 207.140.148.117 **Dest. Port** 80 **Transport** TCP

Artifacts 2 **Packets** 24 **Bytes** 17368 **Timestamp** +225.645s

Network Stream: 53 (HTTP)

Src. IP 192.168.1.148 **Src. Port** 1134 **Dest. IP** 207.140.148.117 **Dest. Port** 80 **Transport** TCP

Artifacts 1 **Packets** 37 **Bytes** 32474 **Timestamp** +225.645s

Network Stream: 54 (HTTP)

Src. IP 192.168.1.148 **Src. Port** 1135 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP

Artifacts 1 **Packets** 747 **Bytes** 806323 **Timestamp** +225.661s

Network Stream: 55 (HTTP)

Src. IP 192.168.1.148 **Src. Port** 1136 **Dest. IP** 207.140.148.117 **Dest. Port** 80 **Transport** TCP

Artifacts 1 **Packets** 41 **Bytes** 33833 **Timestamp** +226.64s

Network Stream: 56 (HTTP)

Src. **Src. Port** 1137 **Dest. IP** 207.140.148.117 **Dest. Port** 80 **Transport** TCP

Network Stream: 57 (HTTP)

Src. **Src. Port** 1138 **Dest. IP** 207.140.148.117 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 2 **Packets** 55 **Bytes** 48213 **Timestamp** +226.696s

Network Stream: 58 (DNS)

Src. **Src. Port** 56990 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 208 **Timestamp** +230.127s

Network Stream: 59 (HTTP)

Src. **Src. Port** 1139 **Dest. IP** 23.32.91.103 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 1 **Packets** 9 **Bytes** 3507 **Timestamp** +230.144s

Network Stream: 60 (DNS)

Src. **Src. Port** 58810 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 217 **Timestamp** +230.265s

Network Stream: 61 (HTTP)

Src. **Src. Port** 1140 **Dest. IP** 165.254.47.113 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 1 **Packets** 14 **Bytes** 9844 **Timestamp** +230.274s

Network Stream: 62 (DNS)

Src. **Src. Port** 61151 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 232 **Timestamp** +230.286s

Network Stream: 63

Src. **Src. Port** 1141 **Dest. IP** 216.58.219.46 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 3 **Packets** 45 **Bytes** 30049 **Timestamp** +230.307s

Network Stream: 64 (DNS)

Src. **Src. Port** 55895 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 276 **Timestamp** +230.315s

Network Stream: 65 (DNS)

Src. **Src. Port** 50056 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 213 **Timestamp** +230.321s

IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 189 **Timestamp** +230.325s

Network Stream: 67 (HTTP)
Src. **Src. Port** 1142 **Dest. IP** 198.232.124.194 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 1 **Packets** 11 **Bytes** 2920 **Timestamp** +230.337s

Network Stream: 68 (DNS)
Src. **Src. Port** 52553 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 180 **Timestamp** +230.34s

Network Stream: 69
Src. **Src. Port** 1143 **Dest. IP** 157.240.11.22 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 2 **Packets** 27 **Bytes** 17314 **Timestamp** +230.36s

Network Stream: 70 (DNS)
Src. **Src. Port** 56164 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 176 **Timestamp** +230.378s

Network Stream: 71 (HTTP)
Src. **Src. Port** 1144 **Dest. IP** 54.192.118.64 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 0 **Packets** 8 **Bytes** 1301 **Timestamp** +230.382s

Network Stream: 72 (HTTP)
Src. **Src. Port** 1145 **Dest. IP** 185.180.13.16 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 2 **Packets** 45 **Bytes** 40968 **Timestamp** +230.395s

Network Stream: 73 (DNS)
Src. **Src. Port** 65118 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 216 **Timestamp** +230.4s

Network Stream: 74
Src. **Src. Port** 1146 **Dest. IP** 23.0.9.250 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 3 **Packets** 20 **Bytes** 13505 **Timestamp** +230.406s

Network Stream: 75 **(HTTP)**

Src. IP 192.168.1.148 **Src. Port** 1147 **Dest. IP** 54.192.117.84 **Dest. Port** 80 **Transport** TCP

Network Stream: 76 **(DNS)**

Src. IP 192.168.1.148 **Src. Port** 59304 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP

Artifacts 0 **Packets** 2 **Bytes** 246 **Timestamp** +230.487s

Network Stream: 77

Src. IP 192.168.1.148 **Src. Port** 1148 **Dest. IP** 216.58.219.46 **Dest. Port** 443 **Transport** TCP

Artifacts 0 **Packets** 28 **Bytes** 13367 **Timestamp** +230.499s

Network Stream: 78

Src. IP 192.168.1.148 **Src. Port** 1149 **Dest. IP** 54.245.92.164 **Dest. Port** 443 **Transport** TCP

Artifacts 0 **Packets** 11 **Bytes** 544 **Timestamp** +230.543s

Network Stream: 79 **(DNS)**

Src. IP 192.168.1.148 **Src. Port** 56738 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP

Artifacts 0 **Packets** 2 **Bytes** 152 **Timestamp** +230.807s

Network Stream: 80 **(HTTP)**

Src. IP 192.168.1.148 **Src. Port** 1150 **Dest. IP** 50.56.156.22 **Dest. Port** 80 **Transport** TCP

Artifacts 1 **Packets** 7 **Bytes** 1550 **Timestamp** +230.81s

Network Stream: 81 **(DNS)**

Src. IP 192.168.1.148 **Src. Port** 64403 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP

Artifacts 0 **Packets** 2 **Bytes** 272 **Timestamp** +230.812s

Network Stream: 82

Src. IP 192.168.1.148 **Src. Port** 1151 **Dest. IP** 54.245.251.207 **Dest. Port** 443 **Transport** TCP

Artifacts 3 **Packets** 25 **Bytes** 11759 **Timestamp** +230.822s

Network Stream: 83 **(DNS)**

Src. IP 192.168.1.148 **Src. Port** 56567 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP

Artifacts 0 **Packets** 2 **Bytes** 224 **Timestamp** +230.83s

Network Stream: 84

Src. IP 192.168.1.148 **Src. Port** 1152 **Dest. IP** 74.125.28.157 **Dest. Port** 443 **Transport** TCP

Artifacts 3 **Packets** 17 **Bytes** 7583 **Timestamp** +230.851s

Network Stream: 85

Src. **Src. Port** 1153 **Dest. IP** 74.125.28.157 **Dest. Port** 443 **Transport** TCP

Network Stream: 86 (DNS)

Src. **Src. Port** 59305 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 148 **Timestamp** +230.994s

Network Stream: 87

Src. **Src. Port** 1154 **Dest. IP** 54.244.236.215 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 4 **Packets** 19 **Bytes** 8180 **Timestamp** +231.009s

Network Stream: 88 (DNS)

Src. **Src. Port** 60601 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 136 **Timestamp** +231.01s

Network Stream: 89

Src. **Src. Port** 1156 **Dest. IP** 216.58.219.36 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 3 **Packets** 15 **Bytes** 5686 **Timestamp** +231.079s

Network Stream: 90

Src. **Src. Port** 1155 **Dest. IP** 216.58.219.36 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 3 **Packets** 15 **Bytes** 5686 **Timestamp** +231.079s

Network Stream: 91 (DNS)

Src. **Src. Port** 58223 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 292 **Timestamp** +231.21s

Network Stream: 92

Src. **Src. Port** 1157 **Dest. IP** 54.245.251.207 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 3 **Packets** 18 **Bytes** 8912 **Timestamp** +231.213s

Network Stream: 93 (DNS)

Src. **Src. Port** 53796 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 301 **Timestamp** +231.354s

Network Stream: 94

Src. **Src. Port** 1158 **Dest. IP** 104.254.150.11 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 2 **Packets** 34 **Bytes** 17051 **Timestamp** +231.373s

IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 161 **Timestamp** +231.544s

Network Stream: 96

Src. **Src. Port** 1159 **Dest. IP** 108.174.10.10 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 2 **Packets** 18 **Bytes** 7165 **Timestamp** +231.555s

Network Stream: 97 (DNS)

Src. **Src. Port** 51784 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 171 **Timestamp** +232.197s

Network Stream: 98

Src. **Src. Port** 1160 **Dest. IP** 52.216.81.112 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 2 **Packets** 23 **Bytes** 5150 **Timestamp** +232.219s

Network Stream: 99

Src. **Src. Port** 1161 **Dest. IP** 52.216.81.112 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 2 **Packets** 23 **Bytes** 5150 **Timestamp** +232.235s

Network Stream: 100 (DNS)

Src. **Src. Port** 60473 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 171 **Timestamp** +232.249s

Network Stream: 101

Src. **Src. Port** 1162 **Dest. IP** 216.58.217.194 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 3 **Packets** 19 **Bytes** 9084 **Timestamp** +232.277s

Network Stream: 102 (HTTP)

Src. **Src. Port** 1164 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 0 **Packets** 345 **Bytes** 340181 **Timestamp** +232.281s

Network Stream: 103 (HTTP)

Src. **Src. Port** 1163 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 0 **Packets** 745 **Bytes** 804435 **Timestamp** +232.281s

Network Stream: 104 (HTTP)

Src. IP 192.168.1.148 **Src. Port** 1165 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP

Network Stream: 105 (HTTP)

Src. IP 192.168.1.148 **Src. Port** 1166 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP

Artifacts 2 **Packets** 731 **Bytes** 703065 **Timestamp** +232.284s

Network Stream: 106 (HTTP)

Src. IP 192.168.1.148 **Src. Port** 1167 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP

Artifacts 0 **Packets** 897 **Bytes** 939717 **Timestamp** +232.284s

Network Stream: 107 (DNS)

Src. IP 192.168.1.148 **Src. Port** 64988 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP

Artifacts 0 **Packets** 2 **Bytes** 239 **Timestamp** +232.332s

Network Stream: 108

Src. IP 192.168.1.148 **Src. Port** 1168 **Dest. IP** 54.245.232.248 **Dest. Port** 443 **Transport** TCP

Artifacts 3 **Packets** 19 **Bytes** 8016 **Timestamp** +232.341s

Network Stream: 109

Src. IP 192.168.1.148 **Src. Port** 1169 **Dest. IP** 54.245.232.248 **Dest. Port** 443 **Transport** TCP

Artifacts 0 **Packets** 16 **Bytes** 3574 **Timestamp** +232.423s

Network Stream: 110

Src. IP 192.168.1.148 **Src. Port** 1170 **Dest. IP** 54.245.92.164 **Dest. Port** 443 **Transport** TCP

Artifacts 0 **Packets** 7 **Bytes** 377 **Timestamp** +234.913s

Network Stream: 111

Src. IP 192.168.1.148 **Src. Port** 1171 **Dest. IP** 54.245.92.164 **Dest. Port** 443 **Transport** TCP

Artifacts 0 **Packets** 7 **Bytes** 344 **Timestamp** +234.968s

Network Stream: 112 (DNS)

Src. IP 192.168.1.148 **Src. Port** 49321 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP

Artifacts 0 **Packets** 2 **Bytes** 208 **Timestamp** +265.096s

Network Stream: 113 (HTTP)

Src. IP 192.168.1.148 **Src. Port** 1172 **Dest. IP** 23.32.91.103 **Dest. Port** 80 **Transport** TCP

Artifacts 0 **Packets** 8 **Bytes** 1229 **Timestamp** +265.158s

Network Stream: 114

Src. **Src. Port** 1173 **Dest. IP** 54.245.92.164 **Dest. Port** 443 **Transport** TCP

Network Stream: 115

Src. **Src. Port** 1174 **Dest. IP** 216.58.219.46 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 3 **Packets** 55 **Bytes** 36511 **Timestamp** +267.168s

Network Stream: 116 (HTTP)

Src. **Src. Port** 1175 **Dest. IP** 54.192.118.64 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 0 **Packets** 8 **Bytes** 1301 **Timestamp** +267.84s

Network Stream: 117

Src. **Src. Port** 1176 **Dest. IP** 157.240.11.22 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 2 **Packets** 26 **Bytes** 17170 **Timestamp** +268.201s

Network Stream: 118

Src. **Src. Port** 1177 **Dest. IP** 54.245.92.164 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 0 **Packets** 7 **Bytes** 377 **Timestamp** +270.939s

Network Stream: 119

Src. **Src. Port** 1178 **Dest. IP** 54.245.92.164 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 0 **Packets** 7 **Bytes** 344 **Timestamp** +271.047s

Network Stream: 120

Src. **Src. Port** 1179 **Dest. IP** 54.245.251.207 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 3 **Packets** 24 **Bytes** 11226 **Timestamp** +278.482s

Network Stream: 121 (HTTP)

Src. **Src. Port** 1180 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 1 **Packets** 360 **Bytes** 340773 **Timestamp** +278.868s

Network Stream: 122 (HTTP)

Src. **Src. Port** 1181 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 1 **Packets** 1214 **Bytes** 1314213 **Timestamp** +278.964s

Network Stream: 123 (HTTP)

Src. **Src. Port** 1182 **Dest. IP** 206.16.239.65 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 0 **Packets** 723 **Bytes** 702711 **Timestamp** +279.019s

IP 192.168.1.148
Artifacts 1 **Packets** 890 **Bytes** 939429 **Timestamp** +279.079s

Network Stream: 125 (DNS)
Src. **Src. Port** 64212 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 235 **Timestamp** +281.385s

Network Stream: 126 (HTTP)
Src. **Src. Port** 1184 **Dest. IP** 165.254.47.107 **Dest. Port** 80 **Transport** TCP
IP 192.168.1.148
Artifacts 0 **Packets** 28 **Bytes** 23566 **Timestamp** +281.39s

Network Stream: 127
Src. **Src. Port** 1185 **Dest. IP** 104.254.150.11 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 2 **Packets** 21 **Bytes** 8172 **Timestamp** +284.876s

Network Stream: 128 (DNS)
Src. **Src. Port** 54498 **Dest. IP** 192.168.1.1 **Dest. Port** 53 **Transport** UDP
IP 192.168.1.148
Artifacts 0 **Packets** 2 **Bytes** 239 **Timestamp** +285.331s

Network Stream: 129
Src. **Src. Port** 1186 **Dest. IP** 54.245.232.248 **Dest. Port** 443 **Transport** TCP
IP 192.168.1.148
Artifacts 3 **Packets** 16 **Bytes** 7895 **Timestamp** +285.427s

Processes

Name: IEXPLORE.EXE
Parent: 13
PID: 14 **Children**: 2 **File Actions**: 20 **Registry Actions**: 48 **Analysis Reason**: Parent is being analyzed

Name: IEXPLORE.EXE
Parent: 14
PID: 16 **Children**: 0 **File Actions**: 103 **Registry Actions**: 2310 **Analysis Reason**: Parent is being analyzed

Name: lsass.exe
Parent: 10
PID: 3 **Children**: 0 **File Actions**: 2 **Registry Actions**: 3 **Analysis Reason**: Process activity after target sample started.

Name: Explorer.EXE

PID: 7 **Children**: 1 **File Actions**: 0 **Registry Actions**: 1 **Analysis Reason**: Process activity after target sample started.

Name: wuauclt.exe

PID: 8 **Children**: 0 **File Actions**: 4 **Registry Actions**: 0 **Analysis Reason**: Process activity after target sample started.

PID: 9 **Children**: 0 **File Actions**: 1 **Registry Actions**: 0 **Analysis Reason**: Process activity after target sample started.

Name: winlogon.exe

PID: 10 **Children**: 1 **File Actions**: 0 **Registry Actions**: 0 **Analysis Reason**: Process activity after target sample started.

Name: ctfmon.exe Parent: 7

PID: 11 **Children**: 0 **File Actions**: 0 **Registry Actions**: 0 **Analysis Reason**: Process activity after target sample started.

Name: wmiprvse.exe

PID: 12 **Children**: 0 **File Actions**: 0 **Registry Actions**: 0 **Analysis Reason**: Process activity after target sample started.

Name: svchost.exe Parent: 4

PID: 13 **Children**: 1 **File Actions**: 0 **Registry Actions**: 0 **Analysis Reason**: Process activity after target sample started.

Name: IEXPLORE.EXE Parent: 14

PID: 15 **Children**: 0 **File Actions**: 28 **Registry Actions**: 1093 **Analysis Reason**: Process activity after target sample started.

Name: svchost.exe Parent: 4

PID: 17 **Children**: 0 **File Actions**: 0 **Registry Actions**: 0 **Analysis Reason**: Process activity after target sample started.

Name: msimn.exe Parent: 1

PID: 6 **Children**: 0 **File Actions**: 6 **Registry Actions**: 109 **Analysis Reason**: Is target sample

Artifacts

Artifact 1: ☐ Gartner Advice - Recognise and Respon...security Threats.eml Related to: artifact 2

Src: submitted **Imports**: 0 **Type**: MHTML - RFC 822 mail, ASCII text, with very long lines **SHA256**: `[illegible]e843be3ad1f1ed145d9437e8eafe16d2bade030ed9040efcef9debc8`
Size: 35418 **Exports**: 0 **AV Sigs**: 0 **MD5**: `d1473949d08da4bf063afbfc1381f73e`

Artifact 2: ☐ Related to: artifact 1

Src: extracted **Imports**: 0 **Type**: HTML - HTML document, UTF-8 Unicode text, with very long ... **SHA256**: `025322ff8648487213b7c210216f8b3b4ca23b811fcee7d35f2fe1c75e46e1b4`
Size: 18830 **Exports**: 0 **AV Sigs**: 0 **MD5**: `dcdd04a4fb233518c422ec39f5991e11`

Artifact 3: ☐ \Documents and Settings\Administrator\Cookies\06PS3W7Y.txt Read by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: TXT - ASCII text **SHA256**: `f4255a22d817c12022f5c081c6c3bd9abc229d6ca161aa8a53d758ef58849de5`
Size: 272 **Exports**: 0 **AV Sigs**: 0 **MD5**: `4cb7e40abc7049e20179b7685f725bcb`

Artifact 4: ☐ \Documents and Settings\Administrator\Cookies\3PWERP0J.txt Created by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: TXT - ASCII text, with very long lines **SHA256**: `107be09eb28eb9c7b44bde9ee93fbb47f1b8659b01ac0d065c8f5d951e1a652e`
Size: 755 **Exports**: 0 **AV Sigs**: 0 **MD5**: `a7883176c54c3933cbc4e3b0ec199fb2`

Artifact 5: ☐ **\Documents and Settings\Administrator\Cookies\5RAO8203.txt**

Src: disk **Imports**: 0 **Type**: TXT - ASCII text **SHA256**: 11e50ace07a0be237c6040f9792926d9b51cd62fff15fb3dea6c67ad7a756c6a
Size: 176 **Exports**: 0 **AV Sigs**: 0 **MD5**: 61c9037b6553554f43c627c2cf2874c2

Src: disk **Imports**: 0 **Type**: TXT - ASCII text **SHA256**: a84b6d614f64d6b56c3c4e6d1ff64432be037faad13b72346e99c0fbda478dc1
Size: 437 **Exports**: 0 **AV Sigs**: 0 **MD5**: c257bafe83da7bec07b8dc50876ad36d

Artifact 7: ☐ **\Documents and Settings\Administrator\Cookies\BCME32JH.txt** Created by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: TXT - ASCII text **SHA256**: 35b7dec5abd4931ebed11508b1c62091464dc2804cc26a018ce1d91fac84c235
Size: 287 **Exports**: 0 **AV Sigs**: 0 **MD5**: 1823b37c4eb68df621803a47746c3e48

Artifact 8: ☐ **\Documents and Settings\Administrator\Cookies\D019I04U.txt** Created by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: TXT - ASCII text **SHA256**: 1f181f03678fd24a07ac6d1778b7a61ce0596419547f1cf96dbd6db8b82f466a
Size: 1032 **Exports**: 0 **AV Sigs**: 0 **MD5**: f24d0e26e6961e096c0169fbc66fa558

Artifact 9: ☐ **\Documents and Settings\Administrator\Cookies\GZIOQ76W.txt**

Src: disk **Imports**: 0 **Type**: TXT - ASCII text **SHA256**: fc8a7bbdaf11498e5ad59fb23e4fbe11fb8af64abb7c7c375ba466789aa1e763
Size: 169 **Exports**: 0 **AV Sigs**: 0 **MD5**: 97dbe979efa6524c85483b1ba9661f86

Artifact 10: ☐ **\Documents and Settings\Administrator\Cookies\OW269EOB.txt**

Src: disk **Imports**: 0 **Type**: TXT - ASCII text **SHA256**: 108b31eb712bab37a76a3d49a023b7701be3504ec3eef89bd0530deffb51f4fa
Size: 239 **Exports**: 0 **AV Sigs**: 0 **MD5**: fade93b8d7af71257946f1594228da58

Artifact 11: ☐ **\Documents and Settings\Administrator... Express\Folders.dbx**

Src: disk **Imports**: 0 **Type**: MS Outlook Express DBX file, folder database **SHA256**: 91adf9ee4dca7d98436e74e33c913adcfb5a1bfcac86544e631b2449c70394ce
Size: 75204 **Exports**: 0 **AV Sigs**: 0 **MD5**: 262a1a8732b143147c266273e78dd2d1

Artifact 12: ☐ **\Documents and Settings\Administrator... Express\Offline.dbx**

Src: disk **Imports**: 0 **Type**: MS Outlook Express DBX file, offline database **SHA256**: 6d13248af99c75db2fb4fa089ac7bc2a4a19e93ec264559e4a3f752f90c69229
Size: 9656 **Exports**: 0 **AV Sigs**: 0 **MD5**: f58d3ff9a6110322ccc1eb4eca91bb0f

Artifact 13: ☐ **\Documents and Settings\Administrator...L\www.gartner[1].xml** Modified by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: ASCII text, with no line terminators **SHA256**: e29bff3eeb1be95ed3851170ff955a099cfcfe9e47cb37e8c4c3b6caf48fcbed
Size: 84 **Exports**: 0 **AV Sigs**: 0 **MD5**: e7cd63d138d284fae39e42d6f8db1f48

Artifact 14: ☐ **\Documents and Settings\Administrator...0B-00506176B712}.dat** Created by: 14 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: CDF - Composite Document File V2 Document, Cannot read se... **SHA256**: 9378c6ed79025baeeb6456d65bccee92d32eaff58d40aa4881
Size: 5632 **Exports**: 0 **AV Sigs**: 0 **MD5**: d564eb11b5d92174a4c425d63813c251

Artifact 15: ☐ **\Documents and Settings\Administrator...0B-00506176B712}.dat** Modified by: 14 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: CDF - Composite Document File V2 Document, Cannot read se... **SHA256**: 54c74e5191834f0a35b41e6c79d177e64b594600607f4fe504c
Size: 4096 **Exports**: 0 **AV Sigs**: 0 **MD5**: b6e0b6177c54dc9c4b084cc79065ae80

Artifact 16: ☐ **\Documents and Settings\Administrator...0B-00506176B712}.dat** Modified by: 14 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: CDF - Composite Document File V2 Document, Cannot read se... **SHA256**: 8ed6a97d9805ace9c28b55534b559538c1637753a0d7fdd0c5
Size: 5120 **Exports**: 0 **AV Sigs**: 0 **MD5**: 7d673357292434c4c289e9280bfdc362

Artifact 17: ☐ **\Documents and Settings\Administrator...0B-00506176B712}.dat** Created by: 14 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: CDF - Composite Document File V2 Document, Cannot read sec **SHA256**: 9661b49e35eb6f10982be60d4ef59b80504cabe4a71d318c9a4
Size: 4096 **Exports**: 0 **AV Sigs**: 0 **MD5**: a3485b8955f42b1358d48b80cd44541b

Artifact 18: ☐ \Documents and Settings\Administrator...0B-00506176B712}.dat Created by: 14 (IEXPLORE.EXE)

Metadata | Behavioral Indicators | Network Activity | Processes | Artifacts | Registry Activity | File Activity

Artifact 19: ☐ \Documents and Settings\Administrator...2320170524\index.dat
Src: disk **Imports**: 0 **Type**: Internet Explorer cache file version Ver 5.2 **SHA256**: 7d44c4e24389ea7486c5b9e62d257c0039289b19e3d39d85d231743d123fd195
Size: 32768 **Exports**: 0 **AV Sigs**: 0 **MD5**: c3e1e782f70e851b8a15c2033e80c7c9

Artifact 20: ☐ \Documents and Settings\Administrator...ngs\Temp\~DF2043.tmp
Src: disk **Imports**: 0 **Type**: **SHA256**: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
Size: 0 **Exports**: 0 **AV Sigs**: 0 **MD5**: d41d8cd98f00b204e9800998ecf8427e

Artifact 21: ☐ \Documents and Settings\Administrator...ngs\Temp\~DFA2EF.tmp
Src: disk **Imports**: 0 **Type**: **SHA256**: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
Size: 0 **Exports**: 0 **AV Sigs**: 0 **MD5**: d41d8cd98f00b204e9800998ecf8427e

Artifact 22: ☐ \Documents and Settings\Administrator...ngs\Temp\~DFC03E.tmp
Src: disk **Imports**: 0 **Type**: **SHA256**: c35020473aed1b4642cd726cad727b63fff2824ad68cedd7ffb73c7cbd890479
Size: 32768 **Exports**: 0 **AV Sigs**: 0 **MD5**: bb7df04e1b0a2570657527a7e108ae23

Artifact 23: ☐ \Documents and Settings\Administrator...ngs\Temp\~DFC051.tmp
Src: disk **Imports**: 0 **Type**: **SHA256**: 076a27c79e5ace2a3d47f9dd2e83e4ff6ea8872b3c2218f66c92b89b55f36560
Size: 512 **Exports**: 0 **AV Sigs**: 0 **MD5**: bf619eac0cdf3f68d496ea9344137e8b

Artifact 24: ☐ \Documents and Settings\Administrator...ngs\Temp\~DFC416.tmp
Src: disk **Imports**: 0 **Type**: **SHA256**: 4fe7b59af6de3b665b67788cc2f99892ab827efae3a467342b3bb4e3bc8e5bfe
Size: 16384 **Exports**: 0 **AV Sigs**: 0 **MD5**: ce338fe6899778aacfc28414f2d9498b

Artifact 25: ☐ \Documents and Settings\Administrator...ngs\Temp\~DFC427.tmp
Src: disk **Imports**: 0 **Type**: **SHA256**: 076a27c79e5ace2a3d47f9dd2e83e4ff6ea8872b3c2218f66c92b89b55f36560
Size: 512 **Exports**: 0 **AV Sigs**: 0 **MD5**: bf619eac0cdf3f68d496ea9344137e8b

Artifact 26: ☐ \Documents and Settings\Administrator...ngs\Temp\~DFC5C5.tmp
Src: disk **Imports**: 0 **Type**: **SHA256**: c35020473aed1b4642cd726cad727b63fff2824ad68cedd7ffb73c7cbd890479
Size: 32768 **Exports**: 0 **AV Sigs**: 0 **MD5**: bb7df04e1b0a2570657527a7e108ae23

Artifact 27: ☐ \Documents and Settings\Administrator...ngs\Temp\~DFC886.tmp
Src: disk **Imports**: 0 **Type**: **SHA256**: 076a27c79e5ace2a3d47f9dd2e83e4ff6ea8872b3c2218f66c92b89b55f36560
Size: 512 **Exports**: 0 **AV Sigs**: 0 **MD5**: bf619eac0cdf3f68d496ea9344137e8b

Artifact 28: ☐ \Documents and Settings\Administrator...HMRCBCR\svrGP[1].gif
Src: disk **Imports**: 0 **Type**: GIF image data, version 89a, 1 x 1 **SHA256**: f1ccea6b7204d9f7913ab45e1afa51d79f83bd4f0319de937b0132e6e02b1aab
Size: 49 **Exports**: 0 **AV Sigs**: 0 **MD5**: dbefe00673f01d8b0f2791f3e30565cc

Artifact 29: ☐ \Documents and Settings\Administrator...HMRCBCR\svrGP[2].gif Created by: 16 (IEXPLORE.EXE)
Src: disk **Imports**: 0 **Type**: GIF image data, version 89a, 1 x 1 **SHA256**: f1ccea6b7204d9f7913ab45e1afa51d79f83bd4f0319de937b0132e6e02b1aab
Size: 49 **Exports**: 0 **AV Sigs**: 0 **MD5**: dbefe00673f01d8b0f2791f3e30565cc

Artifact 30: ☐ **\Documents and Settings\Administrator...ConPro-Medium[1].eot**

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Fakt Con Pro Medium family **SHA256**: 5fd6cd777dfb9f573584b97a8ac8188ceb29ded022321a882a6d66cba6a
Size: 20880 **Exports**: 0 **AV Sigs**: 0 **MD5**: 8418bb0ef68ec6e1b5ccc0465efbe120

Metadata | Behavioral Indicators | Network Activity | Processes | Artifacts | Registry Activity | File Activity

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Fakt Pro Bl... **SHA256**: 24ef7771455eb1dcbfaeb7b3cba975720f941db9c13fe5f6b28da0741e6d63d4
Size: 20341 **Exports**: 0 **AV Sigs**: 0 **MD5**: 99e04d36d88bae6ca1ef0847cadb8222

Artifact 32: ☐ **\Documents and Settings\Administrator...RCBCR\favicon[5].ico**

Src: disk **Imports**: 0 **Type**: MS Windows icon resource - 1 icon, 16x16, 32 bits/pixel **SHA256**: ad184cfba707dce2b25ecfb7bef13bc775949b1cf75d0b0f660f7f3127
Size: 894 **Exports**: 0 **AV Sigs**: 0 **MD5**: 6a6386ee8d17befc46f25bd4687910ed

Artifact 33: ☐ **\Documents and Settings\Administrator...edium-webfont[1].eot**

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Roboto Medium family **SHA256**: 4646396932c3ed852f6946b0149ad7fe3eaca63eb0f507abd4742afa3f1ac1
Size: 21364 **Exports**: 0 **AV Sigs**: 0 **MD5**: 4d9f3f9e5195e7b074bb63ba4ce42208

Artifact 34: ☐ **\Documents and Settings\Administrator...talic-webfont[1].eot**

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Roboto Medium family **SHA256**: dcc1e2ecfd7bd8312723e86086244f3df738c934a43c7d89b0d06f39681709
Size: 24908 **Exports**: 0 **AV Sigs**: 0 **MD5**: 78333c4e825eb31f2117349a350bd4fe

Artifact 35: ☐ **\Documents and Settings\Administrator...Light-webfont[1].eot**

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Roboto Condensed Light family **SHA256**: 59914b2df99a2e7e165e265e22370939ae07fb9494112198e9cc06
Size: 21661 **Exports**: 0 **AV Sigs**: 0 **MD5**: a4481455fde20155f99d9bf866da977d

Artifact 36: ☐ **\Documents and Settings\Administrator...gular-webfont[1].eot**

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Roboto Condensed family **SHA256**: 6210b12b1324fcd446c75a016f4cf0448e53b7a4192b7141178faf14af4
Size: 21712 **Exports**: 0 **AV Sigs**: 0 **MD5**: 01a9358fc6594120b72d4d3c419dc356

Artifact 37: ☐ **\Documents and Settings\Administrator...s;wa20a55a23e6eb8dbd**

Src: disk **Imports**: 0 **Type**: ASCII text, with very long lines **SHA256**: 327d84d78ec09d4b668c10a2b2c3c21ef2188b10b385f9e4a2fa9988c9dba7d3
Size: 6771 **Exports**: 0 **AV Sigs**: 0 **MD5**: c04c71dbaf7bb477aa5394770bc1f88d

Artifact 38: ☐ **\Documents and Settings\Administrator...BCR\8025860307[2].js**

Src: disk **Imports**: 0 **Type**: JS - ASCII text, with very long lines **SHA256**: d9bc161c70f2435b467822f86c619b8fab25ca9d20fc2fc1be7ecba8a4855cef
Size: 11787 **Exports**: 0 **AV Sigs**: 0 **MD5**: 32d49ff915a9960c10c26fc10d763b71

Artifact 39: ☐ **\Documents and Settings\Administrator...ersion_check[1].html**

Src: disk **Imports**: 0 **Type**: ASCII text, with no line terminators **SHA256**: a0690aecd1c75c8cba40cebc743b380c63937503a363f2f04b529e3d1a514155
Size: 24 **Exports**: 0 **AV Sigs**: 0 **MD5**: 97f1da500bb79e67421502f8e88e3141

Artifact 40: ☐ **\Documents and Settings\Administrator...RCBCR\fbevents[1].js** Created by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: JS - ASCII text, with very long lines **SHA256**: 84e7950596b1ea98cf954f1337ee2bdb29a4ec27746a21193468268abe8fcd75
Size: 31547 **Exports**: 0 **AV Sigs**: 0 **MD5**: b7871d762ae6d40944891a4b2e1fa0bb

Artifact 41: ☐ **\Documents and Settings\Administrator...RCBCR\Gartner[1].eot**

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Gartner family **SHA256**: 00d6561e9feb9361b47a1e8bd3ca9e7d795d620124cc10791664959bd92eaee5
Size: 67752 **Exports**: 0 **AV Sigs**: 0 **MD5**: 52717cba0b135a970375983a9ec5bcbf

Artifact 42: ☐ **\Documents and Settings\Administrator...s;wa3c2b0a4c9e7825a4** Modified by: 15 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: ASCII text, with CRLF line terminators **SHA256**: a5af45d23429620bd3aa3b7dc2be0eed45b238870707046d1e7d8d68435ec95f
Size: 6126 **Exports**: 0 **AV Sigs**: 0 **MD5**: 9eba7cc51165d27cd50f98f95ab2222c

Artifact 43: ☐ \Documents and Settings\Administrator...R\hotjar-64884[1].js Read by: 16 (IEXPLORE.EXE)

Artifact 44: ☐ \Documents and Settings\Administrator...s;wa222154262af23e40
Src: disk **Imports**: 0 **Type**: HTML - HTML document, ASCII text, with very long lines **SHA256**: [illegible]0838c161f29e7c46d54fbc044d12cd164baae13255e562c6be3aa91809
Size: 2636 **Exports**: 0 **AV Sigs**: 0 **MD5**: 3044234175ac91f49b03ff999c592b85

Artifact 45: ☐ \Documents and Settings\Administrator...\imagehandler[1].png
Src: disk **Imports**: 0 **Type**: PNG - PNG image data, 200 x 66, 8-bit/color RGBA, non-int... **SHA256**: bf17a0b2a015d8c8a6443bd6a982da667a8c97ee6999552f806ae7e99980f283
Size: 4281 **Exports**: 0 **AV Sigs**: 0 **MD5**: af5c507a7886027fe00011f4ccf7f442

Artifact 46: ☐ \Documents and Settings\Administrator...\imagehandler[2].png
Src: disk **Imports**: 0 **Type**: PNG - PNG image data, 200 x 34, 8-bit/color RGBA, non-int... **SHA256**: 4fe0e5cbfb20f38d3fe2c15c96fbe4bac831d9edec0bf8e59f2cda1739e2c511
Size: 7632 **Exports**: 0 **AV Sigs**: 0 **MD5**: 832cdf0a2f08ef4c2e0d48d89406a231

Artifact 47: ☐ \Documents and Settings\Administrator...\imagehandler[3].png
Src: disk **Imports**: 0 **Type**: PNG - PNG image data, 200 x 70, 8-bit/color RGBA, non-int... **SHA256**: f8d98b2816fb5f5958453f957a32d8eb0b39c632c6f117acdfe11b1ee8d59c5a
Size: 5845 **Exports**: 0 **AV Sigs**: 0 **MD5**: a5f575adba450e206d71fb453eeb4671

Artifact 48: ☐ \Documents and Settings\Administrator...s;wa7234b21e99f75bcf
Src: disk **Imports**: 0 **Type**: ASCII text **SHA256**: 5dcc1f650548dab92380f10aee2a8c4c878ece063b5d4201c1205b3a343f9a8b
Size: 3128 **Exports**: 0 **AV Sigs**: 0 **MD5**: 34259e1b3697ec38ec1ad00f29c64305

Artifact 49: ☐ \Documents and Settings\Administrator...s;wa95bad9e475cfde4d
Src: disk **Imports**: 0 **Type**: ASCII text, with very long lines **SHA256**: 0c853c2cc205bafe5d893017b6a03a2acf0f04a11b85f80605514cf0ae540fe6
Size: 21638 **Exports**: 0 **AV Sigs**: 0 **MD5**: 9ec3c315b67f434aabc4da58eabc6c3a

Artifact 50: ☐ \Documents and Settings\Administrator...1AH\elqCfg.min[1].js Read by: 16 (IEXPLORE.EXE)
Src: disk **Imports**: 0 **Type**: JS - ASCII text, with very long lines, with no line termi... **SHA256**: [illegible]7da15e4829478cbf6712c07a352c5838c9a0799abbfa929ec6af52e43474
Size: 6039 **Exports**: 0 **AV Sigs**: 0 **MD5**: 2b79a76548e03a6dd2f2b548a022a566

Artifact 51: ☐ \Documents and Settings\Administrator...edium-webfont[1].eot Modified by: 16 (IEXPLORE.EXE)
Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Roboto Medium family **SHA256**: [illegible]4646396932c3ed852f6946b0149ad7fe3eaca63eb0f507abd4742afa3f1ac1
Size: 21364 **Exports**: 0 **AV Sigs**: 0 **MD5**: 4d9f3f9e5195e7b074bb63ba4ce42208

Artifact 52: ☐ \Documents and Settings\Administrator...gular-webfont[1].eot
Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Roboto family **SHA256**: cbb656ad18b9fa7d67c2d6e67372be1bc5924f9ad9a708619a31597de23ce8c0
Size: 21320 **Exports**: 0 **AV Sigs**: 0 **MD5**: 30799efa5bf74129468ad4e257551dc3

Artifact 53: ☐ \Documents and Settings\Administrator...\imagehandler[1].jpg
Src: disk **Imports**: 0 **Type**: JPEG - JPEG image data, JFIF standard 1.01, resolution (D... **SHA256**: [illegible]4dd4dae173da1d7c6ab853c1fe372163cdc250301358c9e5fd5df476
Size: 2552 **Exports**: 0 **AV Sigs**: 0 **MD5**: 7a817888b842d3930a5267f31577db8e

Artifact 54: ☐ **\Documents and Settings\Administrator...\imagehandler[1].png**

Src: disk **Imports**: 0 **Type**: PNG - PNG image data, 200 x 80, 8-bit/color RGBA, non-int... **SHA256**: 9315aee0a2852ac41a2579d727d6e1d0893c0cf5a2bf3decbd16c47591a43ff3

Metadata | Behavioral Indicators | Network Activity | Processes | Artifacts | Registry Activity | File Activity

Artifact 55: ☐ **\Documents and Settings\Administrator...\imagehandler[2].png**

Src: disk **Imports**: 0 **Type**: PNG - PNG image data, 200 x 90, 8-bit/color RGBA, non-int... **SHA256**: d698d832e10694facd0aebc1d9fa5a5151856db89c9642ccedf20581f240a16d

Size: 7970 **Exports**: 0 **AV Sigs**: 0 **MD5**: acbf13af74bd1c65f3b77fe8dabe73d4

Artifact 56: ☐ **\Documents and Settings\Administrator...\AD2J21AH\3437[1].js** Read by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: JS - C source, ASCII text, with very long lines, with CRLF line terminators **SHA256**: 7804a67570be2aad497a935514e039fb3a85cdbd360001ccd4553721eb5

Size: 11241 **Exports**: 0 **AV Sigs**: 0 **MD5**: 1e7efaae9fa37c3f7d5ae462c58a2a2a

Artifact 57: ☐ **\Documents and Settings\Administrator...5\AD2J21AH\585951[1]**

Src: disk **Imports**: 0 **Type**: HTML - HTML document, ASCII text, with very long lines, with CRLF line terminators **SHA256**: aa9e585c20ddbe5d50a1d1fab13c1ec0ec316d9eedf341ef2dae7c2

Size: 76082 **Exports**: 0 **AV Sigs**: 0 **MD5**: 0c85f4c2d496a984b25221426a86b741

Artifact 58: ☐ **\Documents and Settings\Administrator...21AH\analytics[1].js** Created by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: JS - ASCII text, with very long lines **SHA256**: e9830d0997e87c328360301ffb0ab81fabd9101f90453976ee61555d6f353af9

Size: 29906 **Exports**: 0 **AV Sigs**: 0 **MD5**: 113986292ce897095c01f51773c88d47

Artifact 59: ☐ **\Documents and Settings\Administrator...ConPro-Medium[1].eot** Read by: 15 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Fakt Con Pro Medium family **SHA256**: dc5fd6cd777dfb9f573584b97a8ac8188ceb29ded022321a882a6d66cba6a

Size: 20880 **Exports**: 0 **AV Sigs**: 0 **MD5**: 8418bb0ef68ec6e1b5ccc0465efbe120

Artifact 60: ☐ **\Documents and Settings\Administrator...FaktPro-Blond[1].eot** Modified by: 15 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Fakt Pro Blond family **SHA256**: 24ef7771455eb1dcbfaeb7b3cba975720f941db9c13fe5f6b28da0741e6d63d4

Size: 20341 **Exports**: 0 **AV Sigs**: 0 **MD5**: 99e04d36d88bae6ca1ef0847cadb8222

Artifact 61: ☐ **\Documents and Settings\Administrator...\FaktPro-Bold[1].eot** Modified by: 15 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Fakt Pro Bold family **SHA256**: b284385f5f97570a054762fe2003bc5d5e83814d5ab1513a84ec6f12add486c3

Size: 21291 **Exports**: 0 **AV Sigs**: 0 **MD5**: 6151189ea5e47236a59c31cc2b06ac29

Artifact 62: ☐ **\Documents and Settings\Administrator...-MediumItalic[1].eot** Modified by: 15 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Fakt Pro Medium family **SHA256**: 851155fe824c96b9780bc0e51c647460da1b7b331019f1efeaa163d5a04e34c3

Size: 21292 **Exports**: 0 **AV Sigs**: 0 **MD5**: fa7c69cbfad361794dd1ca64c352ef7a

Artifact 63: ☐ **\Documents and Settings\Administrator...tPro-SemiBold[1].eot** Created by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Fakt Pro Semibold family **SHA256**: d932d71712de86771b9518ddabad91ebd089116c0c88598e130da0eca5544e7

Size: 20948 **Exports**: 0 **AV Sigs**: 0 **MD5**: 346713f75102d5018260ebfef5b262a2

Artifact 64: ☐ **\Documents and Settings\Administrator...D2J21AH\svrGP[1].gif** Created by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: GIF image data, version 89a, 1 x 1 **SHA256**: f1ccea6b7204d9f7913ab45e1afa51d79f83bd4f0319de937b0132e6e02b1aab

Size: 49 **Exports**: 0 **AV Sigs**: 0 **MD5**: dbefe00673f01d8b0f2791f3e30565cc

Artifact 65: ☐ **\Documents and Settings\Administrator...J21AH\Gartner[1].eot** Created by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Gartner family **SHA256**: 00d6561e9feb9361b47a1e8bd3ca9e7d795d620124cc10791664959bd92eaee5

Size: 67752 **Exports**: 0 **AV Sigs**: 0 **MD5**: 52717cba0b135a970375983a9ec5bcbf

Artifact 66: ☐ \Documents and Settings\Administrator...s;wa3ad28c8ff4ee9447

Src: disk **Imports**: 0 **Type**: HTML - HTML document, ASCII text, with very long lines **SHA256**: ...ea64ed55d41d8700cac136ee3ee86724cf1af68ae9aababd01da135370
Size: 17798 **Exports**: 0 **AV Sigs**: 0 **MD5**: `cfd940cafd8ef26a39f8e0709aa2284b`

Src: disk **Imports**: 0 **Type**: JS - data **SHA256**: `bc3d6f43304d8a6548665a7bb509692bae8d131306b6571441894c0f781cd9e5`
Size: 15337 **Exports**: 0 **AV Sigs**: 0 **MD5**: `8410567ea7209298e5f8f820c43a00fa`

Artifact 68: ☐ \Documents and Settings\Administrator...ontent.IE5\index.dat

Src: disk **Imports**: 0 **Type**: Internet Explorer cache file version Ver 5.2 **SHA256**: `aecd10f68740e3e3e26c157e4d8d0df13afc958a9369bfb00030949592fef2b4`
Size: 52428 **Exports**: 0 **AV Sigs**: 0 **MD5**: `0cee47d1afb8b76c7dfedd72fa783cd0`

Artifact 69: ☐ \Documents and Settings\Administrator...AX\insight.min[1].js Read by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: JS - ASCII text, with very long lines **SHA256**: `b314be9bd5782c13508c0802d599b366f2fa7e2a78909f2eda47db76ed7530f2`
Size: 22455 **Exports**: 0 **AV Sigs**: 0 **MD5**: `67534aa7df24f127de4c55f40c1d8b41`

Artifact 70: ☐ \Documents and Settings\Administrator...E5\MRMBYDAX\u[1].gif

Src: disk **Imports**: 0 **Type**: GIF image data, version 89a, 1 x 1 **SHA256**: `853b983923a033223e4f391790e6e86619b31d542b40e7e1e8221fb0d6957ab1`
Size: 32 **Exports**: 0 **AV Sigs**: 0 **MD5**: `776f5f447e5e03b50f3bc4d4ec78daaa`

Artifact 71: ☐ \Documents and Settings\Administrator...E5\MRMBYDAX\wbk2.tmp Created by: 6 (msimn.exe)

Src: disk **Imports**: 0 **Type**: HTML - HTML document, UTF-8 Unicode text, with very long ... **SHA256**: `399caa09ff46114bc51700963a78c5c8d36b65d8352621b387ad4872082d3b6b`
Size: 18832 **Exports**: 0 **AV Sigs**: 0 **MD5**: `9774363c955eb36b7bd825343f0db192`

Artifact 72: ☐ \Documents and Settings\Administrator...E5\MRMBYDAX\ec[1].js Read by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: JS - ASCII text, with very long lines **SHA256**: `058ed961bfe422af7bfc65865f4c08531ec8ace995f8a1ec560a46581cb7712c`
Size: 2779 **Exports**: 0 **AV Sigs**: 0 **MD5**: `7b430c6350a59a7cf22b9adeccba327b`

Artifact 73: ☐ \Documents and Settings\Administrator...-MediumItalic[1].eot Modified by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Fakt Pro Medium **SHA256**: `851155fe824c96b9780bc0e51c647460da1b7b331019f1efeaa163d5a04e34c3`
Size: 21292 **Exports**: 0 **AV Sigs**: 0 **MD5**: `fa7c69cbfad361794dd1ca64c352ef7a`

Artifact 74: ☐ \Documents and Settings\Administrator...BYDAX\favicon[1].ico

Src: disk **Imports**: 0 **Type**: MS Windows icon resource - 1 icon, 16x16, 32 bits/pixel **SHA256**: `...ad184cfba707dce2b25ecfb7bef13bc775949b1cf75d0b0f660f7f3127`
Size: 894 **Exports**: 0 **AV Sigs**: 0 **MD5**: `6a6386ee8d17befc46f25bd4687910ed`

Artifact 75: ☐ \Documents and Settings\Administrator...-Bold-webfont[1].eot Created by: 15 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Roboto family **SHA256**: `a2ca27e10e7111ca13d7b9368c4b55a165ebf24b40ac16ec715cd3881204bb3a`
Size: 20966 **Exports**: 0 **AV Sigs**: 0 **MD5**: `ecdd509cadbf1ea78b8d2e31ec52328c`

Artifact 76: ☐ \Documents and Settings\Administrator...-Bold-webfont[2].eot

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Roboto family **SHA256**: `a2ca27e10e7111ca13d7b9368c4b55a165ebf24b40ac16ec715cd3881204bb3a`
Size: 20966 **Exports**: 0 **AV Sigs**: 0 **MD5**: `ecdd509cadbf1ea78b8d2e31ec52328c`

Artifact 77: ☐ \Documents and Settings\Administrator...Light-webfont[1].eot Created by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Roboto Light **SHA256**: `2517b97e2c0e1e6c8ceb9dd007015f897926bc504154137281eec4c1a9f9bdc9`
Size: 20940 **Exports**: 0 **AV Sigs**: 0 **MD5**: `a990f611f2305dc12965f186c2ef2690`

Artifact 78: ☐ **\Documents and Settings\Administrator...gular-webfont[1].eot**

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Roboto fam... **SHA256**: cbb656ad18b9fa7d67c2d6e67372be1bc5924f9ad9a708619a31597de23ce8c0
Size: 21320 **Exports**: 0 **AV Sigs**: 0 **MD5**: 30799efa5bf74129468ad4e257551dc3

Metadata | Behavioral Indicators | Network Activity | Processes | Artifacts | Registry Activity | File Activity

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Roboto Thin **SHA256**: ec8252b3a3f3a07433ad90409b707abd59b88f74dae0878ea97dd4d5357ea5ae
Size: 21659 **Exports**: 0 **AV Sigs**: 0 **MD5**: dfe56a876d0282555d1e2458e278060f

Artifact 80: ☐ **\Documents and Settings\Administrator...-Thin-webfont[2].eot**

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Roboto Thin **SHA256**: ec8252b3a3f3a07433ad90409b707abd59b88f74dae0878ea97dd4d5357ea5ae
Size: 21659 **Exports**: 0 **AV Sigs**: 0 **MD5**: dfe56a876d0282555d1e2458e278060f

Artifact 81: ☐ **\Documents and Settings\Administrator...BYDAX\gartner[1].png**

Src: disk **Imports**: 0 **Type**: PNG - PNG image data, 96 x 22, 8-bit/color RGBA, non-inte... **SHA256**: 2f6e8c477c0a9d77b4831699748f75ea700f0ad4ed48f65e7489a5279bd9ee39
Size: 2680 **Exports**: 0 **AV Sigs**: 0 **MD5**: b8519e448f1cd4ce5a58a35e0c931a7b

Artifact 82: ☐ **\Documents and Settings\Administrator...E5\MRMBYDAX\CAZW7A43** Created by: 6 (msimn.exe)

Src: disk **Imports**: 0 **Type**: **SHA256**: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
Size: 0 **Exports**: 0 **AV Sigs**: 0 **MD5**: d41d8cd98f00b204e9800998ecf8427e

Artifact 83: ☐ **\Documents and Settings\Administrator...AX\respond.min[1].js** Modified by: 15 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: JS - HTML document, ASCII text, with very long lines **SHA256**: [illegible]8807ef669fa70d0d9375347f5552897f76c6ae8e2e6f97ef592595462d8d1
Size: 4377 **Exports**: 0 **AV Sigs**: 0 **MD5**: afc1984a3d17110449dc90cf22de0c27

Artifact 84: ☐ **\Documents and Settings\Administrator...RMBYDAX\svrGP[1].gif**

Src: disk **Imports**: 0 **Type**: GIF image data, version 89a, 1 x 1 **SHA256**: f1ccea6b7204d9f7913ab45e1afa51d79f83bd4f0319de937b0132e6e02b1aab
Size: 49 **Exports**: 0 **AV Sigs**: 0 **MD5**: dbefe00673f01d8b0f2791f3e30565cc

Artifact 85: ☐ **\Documents and Settings\Administrator...5\MRMBYDAX\gtm[1].js**

Src: disk **Imports**: 0 **Type**: JS - ASCII text, with very long lines **SHA256**: 19b0828827277afed21d089c159d28f050001aa1474dc5db65099b13f74f332a
Size: 168769 **Exports**: 0 **AV Sigs**: 0 **MD5**: 663cc6cc044d6f69310dec1f059f3c85

Artifact 86: ☐ **\Documents and Settings\Administrator...\imagehandler[1].jpg**

Src: disk **Imports**: 0 **Type**: JPEG - JPEG image data, JFIF standard 1.01, resolution (D... **SHA256**: [illegible]4196cd5e40b30730ab1bb64eb08f9010c1032ff405ff99921f23bce
Size: 3593 **Exports**: 0 **AV Sigs**: 0 **MD5**: 8fefbff472d94e69d57b7026c74c82ff

Artifact 87: ☐ **\Documents and Settings\Administrator...\imagehandler[1].png**

Src: disk **Imports**: 0 **Type**: PNG - PNG image data, 200 x 80, 8-bit/color RGBA, non-int... **SHA256**: a301d58bb0a5885f4e018b3d3df872d64f30fc3294b32fdc2f38c1ad5d8a02ce
Size: 6419 **Exports**: 0 **AV Sigs**: 0 **MD5**: e62807bc364354313764c7e87bf3215d

Artifact 88: ☐ **\Documents and Settings\Administrator...\imagehandler[2].jpg**

Src: disk **Imports**: 0 **Type**: JPEG - JPEG image data, Exif standard: [illegible]mage data, **SHA256**: [illegible]374cfe2544a0e6d0b204146425261b9112448b8636c1476b4156432f8
Size: 20237 **Exports**: 0 **AV Sigs**: 0 **MD5**: 1c1348805d4f6f11311707b171f71350

Artifact 89: ☐ **\Documents and Settings\Administrator...ecurity-india[1].htm** Created by: 15 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: HTML - HTML document, UTF-8 Unicode text, with very long ... **SHA256**: 518c7dfb398caf876e8d5c658bbaa0a6075c52f9316fab2585283696ea4b6569

Size: 14336 **Exports**: 0 **AV Sigs**: 0 **MD5**: 4f34ba867c91f6b9ce7f4ffedbf5db73

Artifact 90: ☐ **\Documents and Settings\Administrator...ecurity-india[2].htm** Modified by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: HTML - HTML document, UTF- **SHA256**: c3422d2c1e56de5531a0ab8fc88f45e49b917c9a38b188788f533fea1d8e8c16

Artifact 91: ☐ **\Documents and Settings\Administrator...\loading-grey[1].gif** Read by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: GIF image data, version 89a, 200 x 200 **SHA256**: 60422d7c04d9fc10efade27c7ffc16a931321fb2c0098f7f733df60e8964c088

Size: 26961 **Exports**: 0 **AV Sigs**: 0 **MD5**: 41e421d4fec6e4277d65556481d76ab4

Artifact 92: ☐ **\Documents and Settings\Administrator...YDAX\main.min[2].css** Modified by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: ASCII text, with very long lines, with no line terminators **SHA256**: 21d993e1c84f87908a294eff55897c253ce3a1d8a90fed253839b6dbdd239e90

Size: 22586 **Exports**: 0 **AV Sigs**: 0 **MD5**: a9127362791442469d0df13221d44be8

Artifact 93: ☐ **\Documents and Settings\Administrator...s;wa58ebf4f94787f212**

Src: disk **Imports**: 0 **Type**: HTML - HTML document, ASCII text, with very long lines, wi... **SHA256**: bf8cbf390a99c94defcefea2f450711a78303548096cea094a6307e

Size: 62943 **Exports**: 0 **AV Sigs**: 0 **MD5**: c05399a53634bf000c6e97d1b6e141cd

Artifact 94: ☐ **\Documents and Settings\Administrator...tPro-SemiBold[1].eot** Modified by: 15 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Fakt Pro SemiBold family **SHA256**: d932d71712de86771b9518ddabad91ebd089116c0c88598e130da0eca5544e7

Size: 20948 **Exports**: 0 **AV Sigs**: 0 **MD5**: 346713f75102d5018260ebfef5b262a2

Artifact 95: ☐ **\Documents and Settings\Administrator...\FaktPro-Thin[1].eot**

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Fakt Pro Thin family **SHA256**: d9ad20b39d155d0bd6b8a1e333c97b42d5dfb7a96062cf6aac9d939e6d5add28

Size: 19960 **Exports**: 0 **AV Sigs**: 0 **MD5**: 4453ac26a588ae2d5b71e7338ad0c40f

Artifact 96: ☐ **\Documents and Settings\Administrator...s;wa72cbcc36dacf519c**

Src: disk **Imports**: 0 **Type**: ASCII text, with very long lines **SHA256**: 24cc29533598f962823c4229bc280487646a27a42a95257c31de1b9b18f3710f

Size: 31819 **Exports**: 0 **AV Sigs**: 0 **MD5**: abda843684d022f3bc22bc83927fe05f

Artifact 97: ☐ **\Documents and Settings\Administrator...\imagehandler[1].jpg**

Src: disk **Imports**: 0 **Type**: JPEG - JPEG image data, JFIF standard 1.02, resolution (D... **SHA256**: 6428859c9d9cd12acfe23f1f207c51c7371a74a3d3afefea644982f8

Size: 2247 **Exports**: 0 **AV Sigs**: 0 **MD5**: a52e761a58a5a0dcd43c508b59d908d7

Artifact 98: ☐ **\Documents and Settings\Administrator...\imagehandler[1].png**

Src: disk **Imports**: 0 **Type**: PNG - PNG image data, 200 x 22, 8-bit/color RGBA, non-int... **SHA256**: 78bc156e16239627d8130f88c7a4aad54c1e2158eba5cb0c283cd6b82bff810c

Size: 5638 **Exports**: 0 **AV Sigs**: 0 **MD5**: 6a5646eaf14e3eb564a11e728ce2dc23

Artifact 99: ☐ **\Documents and Settings\Administrator...\imagehandler[2].png**

Src: disk **Imports**: 0 **Type**: PNG - PNG image data, 200 x 74, 8-bit/color RGBA, non-int... **SHA256**: 81278e76a448414c46166ad39d2df4e650472f76b4f94a178b28d2f3fdde39e8

Size: 7502 **Exports**: 0 **AV Sigs**: 0 **MD5**: 02038586cedbe9be7cfcf56d60867af9

Artifact 100: ☐ **\Documents and Settings\Administrator...s;wa480a643f34f8b8be**

Src: disk **Imports**: 0 **Type**: ASCII text, with very long lines **SHA256**: 540bc6dec1dd4b92ea4d3fb903f69eabf6d919afd48f4e312b163c28cff0f441

Size: 95786 **Exports**: 0 **AV Sigs**: 0 **MD5**: 8101d596b2b8fa35fe3a634ea342d7c3

Artifact 101: ☐ **\Documents and Settings\Administrator...V4HU7MN\svrGP[1].gif** Created by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: GIF image data, version 89a, 1 x 1 **SHA256**: f1ccea6b7204d9f7913ab45e1afa51d79f83bd4f0319de937b0132e6e02b1aab
Size: 49 **Exports**: 0 **AV Sigs**: 0 **MD5**: dbefe00673f01d8b0f2791f3e30565cc

Artifact 102: ☐ \Documents and Settings\Administrator...E5\MV4HU7MN\s[1].gif

Metadata | Behavioral Indicators | Network Activity | Processes | Artifacts | Registry Activity | File Activity

Artifact 103: ☐ \Documents and Settings\Administrator...N\coupon_code1[1].js Read by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: JS - ASCII text, with very long lines, with **SHA256**: …bea0989e210a4fcb108862440ecfc2068675e4e028be60223242005d4c1c
Size: 1968 **Exports**: 0 **AV Sigs**: 0 **MD5**: f784887fc7a324d938310f731ed76ad1

Artifact 104: ☐ \Documents and Settings\Administrator...Light-webfont[1].eot

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Roboto Lig **SHA256**: 2517b97e2c0e1e6c8ceb9dd007015f897926bc504154137281eec4c1a9f9bdc9
Size: 20940 **Exports**: 0 **AV Sigs**: 0 **MD5**: a990f611f2305dc12965f186c2ef2690

Artifact 105: ☐ \Documents and Settings\Administrator...talic-webfont[1].eot

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Roboto Me **SHA256**: …dcc1e2ecfd7bd8312723e86086244f3df738c934a43c7d89b0d06f39681709
Size: 24908 **Exports**: 0 **AV Sigs**: 0 **MD5**: 78333c4e825eb31f2117349a350bd4fe

Artifact 106: ☐ \Documents and Settings\Administrator...Light-webfont[1].eot Created by: 15 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Roboto Co **SHA256**: …59914b2df99a2e7e165e265e22370939ae07fb9494112198e9cc06
Size: 21661 **Exports**: 0 **AV Sigs**: 0 **MD5**: a4481455fde20155f99d9bf866da977d

Artifact 107: ☐ \Documents and Settings\Administrator...gular-webfont[1].eot Created by: 15 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: Embedded OpenType (EOT), Roboto Co **SHA256**: …6210b12b1324fcd446c75a016f4cf0448e53b7a4192b7141178faf14af4
Size: 21712 **Exports**: 0 **AV Sigs**: 0 **MD5**: 01a9358fc6594120b72d4d3c419dc356

Artifact 108: ☐ \Documents and Settings\Administrator...U7MN\roundtrip[1].js Read by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: JS - ASCII text, with very long lines **SHA256**: 3be80e5456069776ab99ca070ac2639249b0079f51bc34357872d106ad9d0c23
Size: 25239 **Exports**: 0 **AV Sigs**: 0 **MD5**: fdefd0b22ea1cab41a933d8678646088

Artifact 109: ☐ \Documents and Settings\Administrator...5\MV4HU7MN\585951[1] Read by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: HTML - HTML document, ASCII text, wi **SHA256**: …aa9e585c20ddbe5d50a1d1fab13c1ec0ec316d9eedf341ef2dae7c2
Size: 76082 **Exports**: 0 **AV Sigs**: 0 **MD5**: 0c85f4c2d496a984b25221426a86b741

Artifact 110: ☐ \Documents and Settings\Administrator...5\MV4HU7MN\585951[2] Created by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: HTML - HTML document, ASCII text, wi **SHA256**: …aa9e585c20ddbe5d50a1d1fab13c1ec0ec316d9eedf341ef2dae7c2
Size: 76082 **Exports**: 0 **AV Sigs**: 0 **MD5**: 0c85f4c2d496a984b25221426a86b741

Artifact 111: ☐ \Documents and Settings\Administrator...V4HU7MN\linkid[1].js Read by: 16 (IEXPLORE.EXE)

Src: disk **Imports**: 0 **Type**: JS - ASCII text, with very long lines **SHA256**: 92fca55833f48b4289ac8f1cedd48752b580fce4ec4b5d81670b8193d6e51b54
Size: 1569 **Exports**: 0 **AV Sigs**: 0 **MD5**: 0cc3a63fe10060af4a349e5df666eefe

Artifact 112: ☐ \Documents and Settings\Administrator...\loading-grey[1].gif

Src: disk **Imports**: 0 **Type**: GIF image data, version 89a, 200 x 200 **SHA256**: 60422d7c04d9fc10efade27c7ffc16a931321fb2c0098f7f733df60e8964c088
Size: 26961 **Exports**: 0 **AV Sigs**: 0 **MD5**: 41e421d4fec6e4277d65556481d76ab4

Artifact 113: ☐ \TEMP\Gartner Advice - Recognise and ...security Threats.eml Related to: artifact 261

Src: disk **Imports**: 0 **Type**: MHTML - RFC 822 mail, ASCII text, with **SHA256**: …f843be3ad1f1ed145d9437e8eafe16d2bade030ed9040efcef9debc8
Size: 35418 **Exports**: 0 **AV Sigs**: 0 **MD5**: d1473949d08da4bf063afbfc1381f73e

Artifact 114: ☐ **\WINDOWS\SoftwareDistribution\DataStore\DataStore.edb** Modified by: 8 (wuauclt.exe)

Src: disk **Imports**: 0 **Type**: Extensible storage engine DataBase, ver…, checks… **SHA256**: [illegible]e8db2e7aaa09e6c79796912ad46ffdb7be21cefdba88fba9238870
Size: 15736832 **Exports**: 0 **AV Sigs**: 0 **MD5**: eb6209911049690c1d414576f7f3df68

Metadata | Behavioral Indicators | Network Activity | Processes | Artifacts | Registry Activity | File Activity

Src: disk **Imports**: 0 **Type**: data **SHA256**: a446186fd701ece351ca44039d9b86ec6229f562d5f22b7aa658a387ab56077c
Size: 8192 **Exports**: 0 **AV Sigs**: 0 **MD5**: de6010fca5e9339175148a9bfd73ba8b

Artifact 116: ☐ **\WINDOWS\SoftwareDistribution\DataStore\Logs\edb.log** Modified by: 8 (wuauclt.exe)

Src: disk **Imports**: 0 **Type**: data **SHA256**: cd968171d211f8d15e6e7210441c8bc706b0b6951c2c1597e91205e7a8dd46a0
Size: 131072 **Exports**: 0 **AV Sigs**: 0 **MD5**: 315b1c711ab7a0129b6f0110632705ba

Artifact 117: ☐ **\WINDOWS\system32\config\SysEvent.Evt**

Src: disk **Imports**: 0 **Type**: data **SHA256**: 1bdc9a8f861d22fc12dd7c9df5afa0a19ccf590b45776b87f5e2b0f94748e87b
Size: 196608 **Exports**: 0 **AV Sigs**: 0 **MD5**: 744aa0f589bac2182c58f1b554b2735d

Artifact 118: ☐ **\WINDOWS\system32\config\WindowsPowerShell.evt**

Src: disk **Imports**: 0 **Type**: data **SHA256**: f43118b275a8d3da45a4d4bfb9c4d599d62e62e3763d411b36049b7aed9dbde1
Size: 65536 **Exports**: 0 **AV Sigs**: 0 **MD5**: c89f5f71a93a424cdaf2890aa5f070b3

Artifact 119: ☐ **certificate-124.cer** Related to: stream 82

Src: network **Imports**: 0 **Type**: data **SHA256**: 48202a7e3ca9b2cc39e6ef3a805018596df742a56663916aa0aa25070b40ec8d
Size: 2867 **Exports**: 0 **AV Sigs**: 0 **MD5**: 3dc9b3852ce005382444a7bb782679c4

Artifact 120: ☐ **mumbai.png** Related to: stream 11

Src: network **Imports**: 0 **Type**: PNG - PNG image data, 1170 x 517, 8-bit/color RGB, non-in... **SHA256**: e4de2ba5c2c3783c19f8968a7cedba0ba354e17d5fc0b80c201a1ddd72ce4528
Size: 67468 **Exports**: 0 **AV Sigs**: 0 **MD5**: 1489c860236e4dfaa0d897142e04ef03

Artifact 121: ☐ **imagehandler.ashx** Related to: stream 51

Src: network **Imports**: 0 **Type**: PNG - PNG image data, 200 x 70, 8-bit/color RGBA, non-int... **SHA256**: f8d98b2816fb5f5958453f957a32d8eb0b39c632c6f117acdfe11b1ee8d59c5a
Size: 5845 **Exports**: 0 **AV Sigs**: 0 **MD5**: a5f575adba450e206d71fb453eeb4671

Artifact 122: ☐ **certificate-165.cer** Related to: stream 108

Src: network **Imports**: 0 **Type**: data **SHA256**: 4348a0e9444c78cb265e058d5e8944b4d84f9662bd26db257f8934a443c70161
Size: 947 **Exports**: 0 **AV Sigs**: 0 **MD5**: 79e4a9840d7d3a96d7c04fe2434c892e

Artifact 123: ☐ **certificate-161.cer** Related to: stream 99

Src: network **Imports**: 0 **Type**: data **SHA256**: f9690880819f06cdcc0b2f224b207f2af6003fb57339b8679a160fa95208d62d
Size: 1127 **Exports**: 0 **AV Sigs**: 0 **MD5**: b1349906c8ccc2a93df7e9a2c395ec6e

Artifact 124: ☐ **security_breach_header.jpg;wa7f1fe461a1b7eb71** Related to: stream 54

Src: network **Imports**: 0 **Type**: JPEG - JPEG image data, JFIF standard…, aspect ratio… **SHA256**: …da0da262e0c0f144dc70fbff8de3fb0aec4a647aa9dc3f57e430f3a5
Size: 77236 **Exports**: 0 **AV Sigs**: 0 **MD5**: 7ce12a38d0b3dc4f8da2b4f7eb22ea0a

Artifact 125: ☐ **seci3_summit_overview_hero.jpg;wa29a580e00b45c795** Related to: stream 43

Src: network **Imports**: 0 **Type**: JPEG - JPEG image data, JFIF standard…, aspect ratio… **SHA256**: …7491659ce6562a347c95c1cf900685ddc17f0188365a0cfff681434
Size: 11797 **Exports**: 0 **AV Sigs**: 0 **MD5**: 31f3635e4a3bf9773c8bf53585fd60f8

Artifact 126: ☐ contu-ruggero.png;waa9f67c5d5a462be0 Related to: stream 45

Src: network **Imports**: 0 **Type**: PNG - PNG image data, 285 x 285, 8-bit/color RGBA, non-in... **SHA256**: c86dedfa2a88417bce1198cbc4df1d04ef459057e41f3fd0f850393858923b9f

Artifact 127: ☐ certificate-129.cer

Src: network **Imports**: 0 **Type**: data **SHA256**: 3c35cc963eb004451323d3275d05b353235053490d9cd83729a2faf5e7ca1cc0
Size: 897 **Exports**: 0 **AV Sigs**: 0 **MD5**: 2e7db2a31d0e3da4b25f49b9542a2e1a

Artifact 128: ☐ RobotoCondensed-Light-webfont.eot Related to: stream 20

Src: network **Imports**: 0 **Type**: Embedded OpenType (EOT), Roboto Condensed Light family **SHA256**: 59914b2df99a2e7e165e265e22370939ae07fb9494112198e9cc06
Size: 21661 **Exports**: 0 **AV Sigs**: 0 **MD5**: a4481455fde20155f99d9bf866da977d

Artifact 129: ☐ certificate-194.cer Related to: stream 129

Src: network **Imports**: 0 **Type**: data **SHA256**: 48202a7e3ca9b2cc39e6ef3a805018596df742a56663916aa0aa25070b40ec8d
Size: 2867 **Exports**: 0 **AV Sigs**: 0 **MD5**: 3dc9b3852ce005382444a7bb782679c4

Artifact 130: ☐ Roboto-Bold-webfont.eot Related to: stream 19

Src: network **Imports**: 0 **Type**: Embedded OpenType (EOT), Roboto family **SHA256**: a2ca27e10e7111ca13d7b9368c4b55a165ebf24b40ac16ec715cd3881204bb3a
Size: 20966 **Exports**: 0 **AV Sigs**: 0 **MD5**: ecdd509cadbf1ea78b8d2e31ec52328c

Artifact 131: ☐ certificate-131.cer Related to: stream 85

Src: network **Imports**: 0 **Type**: data **SHA256**: 2fcd4615df0eabffb237102b1c49065cf3ca8e8e42fb282ac26d5e124047ee59
Size: 1366 **Exports**: 0 **AV Sigs**: 0 **MD5**: ac722e2055b18eb6264c320de894d7d8

Artifact 132: ☐ certificate-158.cer Related to: stream 98

Src: network **Imports**: 0 **Type**: data **SHA256**: 659a3d7684850e6d664f5131f9f8765469b9c7017b7a0e206f8c1c9445cb1c69
Size: 1374 **Exports**: 0 **AV Sigs**: 0 **MD5**: 0189e7cdef655f5f6d5745c1ac8fad24

Artifact 133: ☐ FaktPro-Blond.eot Related to: stream 22

Src: network **Imports**: 0 **Type**: Embedded OpenType (EOT), Fakt Pro Blond family **SHA256**: 24ef7771455eb1dcbfaeb7b3cba975720f941db9c13fe5f6b28da0741e6d63d4
Size: 20341 **Exports**: 0 **AV Sigs**: 0 **MD5**: 99e04d36d88bae6ca1ef0847cadb8222

Artifact 134: ☐ imagehandler.ashx Related to: stream 56

Src: network **Imports**: 0 **Type**: JPEG - JPEG image data, JFIF standard 1.01, resolution (D... **SHA256**: 4dd4dae173da1d7c6ab853c1fe372163cdc250301358c9e5fd5df476
Size: 2552 **Exports**: 0 **AV Sigs**: 0 **MD5**: 7a817888b842d3930a5267f31577db8e

Artifact 135: ☐ certificate-157.cer Related to: stream 101

Src: network **Imports**: 0 **Type**: data **SHA256**: 3c35cc963eb004451323d3275d05b353235053490d9cd83729a2faf5e7ca1cc0
Size: 897 **Exports**: 0 **AV Sigs**: 0 **MD5**: 2e7db2a31d0e3da4b25f49b9542a2e1a

Artifact 136: ☐ certificate-159.cer Related to: stream 98

Src: network **Imports**: 0 **Type**: data **SHA256**: f9690880819f06cdcc0b2f224b207f2af6003fb57339b8679a160fa95208d62d
Size: 1127 **Exports**: 0 **AV Sigs**: 0 **MD5**: b1349906c8ccc2a93df7e9a2c395ec6e

Artifact 137: ☐ smarter-with-gartner Related to: stream 22

Src: network **Imports**: 0 **Type**: HTML - HTML document, UTF-8 Unicode text, with very long ... **SHA256**: da45cc2e0ebfc79f0d80d281f8e8f14a38cb2e3b100abf061265f110db39a627
Size: 15525 **Exports**: 0 **AV Sigs**: 0 **MD5**: 461bb48fadd2a914de1867bc238befb4

Artifact 138: ☐ modernizr.custom.93545.js;wa3ad28c8ff4ee9447 Related to: stream 19

Src: network **Imports**: 0 **Type**: HTML - HTML document, ASCII text, with very long lines **SHA256**: ea64ed55d41d8700cac136ee3ee86724cf1af68ae9aababd01da135370
Size: 17798 **Exports**: 0 **AV Sigs**: 0 **MD5**: cfd940cafd8ef26a39f8e0709aa2284b

Metadata | Behavioral Indicators | Network Activity | Processes | Artifacts | Registry Activity | File Activity

Src: network **Imports**: 0 **Type**: data **SHA256**: 9f630426df1d8abfd80ace98871ba833ab9742cb34838de2b5285ed54c0c7dcc
Size: 1012 **Exports**: 0 **AV Sigs**: 0 **MD5**: c56f1a63b817b7318934c06ec5abb5b3

Artifact 140: ☐ jquery-1.11.1.min.js;wa480a643f34f8b8be Related to: stream 11

Src: network **Imports**: 0 **Type**: ASCII text, with very long lines **SHA256**: 540bc6dec1dd4b92ea4d3fb903f69eabf6d919afd48f4e312b163c28cff0f441
Size: 95786 **Exports**: 0 **AV Sigs**: 0 **MD5**: 8101d596b2b8fa35fe3a634ea342d7c3

Artifact 141: ☐ color_band_4.png Related to: stream 21

Src: network **Imports**: 0 **Type**: PNG - PNG image data, 965 x 528, 8-bit/color RGBA, non-in... **SHA256**: a9062d6a1d60a2eaf4dd4f1d9848ac4bd16dc28667abc9efb3238b8c96945156
Size: 37949 **Exports**: 0 **AV Sigs**: 0 **MD5**: eb2595e699fad9b17debcb06a431e29d

Artifact 142: ☐ your-first-100-days-as-a-new-chief-in...g;wa5fe005b93418358d Related to: stream 124

Src: network **Imports**: 0 **Type**: JPEG - JPEG image data, JFIF standard 1.01, aspect ratio, **SHA256**: e664e1bf5c042d85fe6e09736afbaa0dc17823db0e91d7aa3acdc2
Size: 90153 **Exports**: 0 **AV Sigs**: 0 **MD5**: c8f549a3d4bb46608430baa4163b42c4

Artifact 143: ☐ FaktPro-Bold.eot Related to: stream 11

Src: network **Imports**: 0 **Type**: Embedded OpenType (EOT), Fakt Pro Bold **SHA256**: b284385f5f97570a054762fe2003bc5d5e83814d5ab1513a84ec6f12add486c3
Size: 21291 **Exports**: 0 **AV Sigs**: 0 **MD5**: 6151189ea5e47236a59c31cc2b06ac29

Artifact 144: ☐ securecloud_header.jpg;wa35c3d475c029782c Related to: stream 105

Src: network **Imports**: 0 **Type**: JPEG - JPEG image data, JFIF standard 1.01, aspect ratio, **SHA256**: 285c21e3bcaa1fdb25792d827b01cd12eef0c2d53763f27591d4c4
Size: 39883 **Exports**: 0 **AV Sigs**: 0 **MD5**: a2ec7952b9927cc8e781552ef3372f99

Artifact 145: ☐ elqCfg.min.js Related to: stream 59

Src: network **Imports**: 0 **Type**: JS - ASCII text, with very long lines, with CRLF, LF line terminators **SHA256**: 7da15e4829478cbf6712c07a352c5838c9a0799abbfa929ec6af52e43474
Size: 6039 **Exports**: 0 **AV Sigs**: 0 **MD5**: 2b79a76548e03a6dd2f2b548a022a566

Artifact 146: ☐ certificate-139.cer Related to: stream 89

Src: network **Imports**: 0 **Type**: data **SHA256**: f43e11723d72f2fa249e0a253fa62c201fb966dd2cf93d3d3dba070290ea01e3
Size: 1156 **Exports**: 0 **AV Sigs**: 0 **MD5**: ccf621f4b1ac33f88716cd147e3d5ca7

Artifact 147: ☐ speaker_tom_scholtz.jpg;wa7ce2a838af55fc13 Related to: stream 45

Src: network **Imports**: 0 **Type**: JPEG - JPEG image data, JFIF standard 1.01, aspect ratio, **SHA256**: ca7e266cba8e9186275049c9aecfef83f44ec41480bd402ca00220b1
Size: 11059 **Exports**: 0 **AV Sigs**: 0 **MD5**: d7ec19ef2fa74a7fd989f5c5b6d37c92

Artifact 148: ☐ er Related to: stream 7

Src: network **Imports**: 0 **Type**: HTML - HTML document, ASCII text, with CRLF, LF line terminators **SHA256**: c9edc40136011c2d26f7f91876521279519555ac7f2d3ebd439
Size: 370 **Exports**: 0 **AV Sigs**: 0 **MD5**: 23424e5d03f61077e84c6b551454fd8a

Artifact 149: ☐ swg_security_landscape_header.jpg;wa649e949be2fb69a8 Related to: stream 122

Src: network **Imports**: 0 **Type**: JPEG - JPEG image data, JFIF standard 1.01, aspect ratio, **SHA256**: cf5608f9e07d1f8a1d585988755e1a955dd2927b6c41324441e2943
Size: 126336 **Exports**: 0 **AV Sigs**: 0 **MD5**: 330957fc894a7dd4ac56041b2d28749f

Artifact 150: ☐ certificate-181.cer
Related to: stream 120

Src: network **Imports**: 0 **Type**: data
Size: 2867 **Exports**: 0 **AV Sigs**: 0
SHA256: 48202a7e3ca9b2cc39e6ef3a805018596df742a56663916aa0aa25070b40ec8d
MD5: 3dc9b3852ce005382444a7bb782679c4

Src: network **Imports**: 0 **Type**: Embedded OpenType (EOT), Fakt Pro Medium family
SHA256: 851155fe824c96b9780bc0e51c647460da1b7b331019f1efeaa163d5a04e34c3
Size: 21292 **Exports**: 0 **AV Sigs**: 0
MD5: fa7c69cbfad361794dd1ca64c352ef7a

Artifact 152: ☐ imagehandler.ashx
Related to: stream 57

Src: network **Imports**: 0 **Type**: JPEG - JPEG image data, Exif standard: [TIFF image data, ...
SHA256: ...74cfe2544a0e6d0b204146425261b9112448b8636c1476b4156432f8
Size: 20237 **Exports**: 0 **AV Sigs**: 0
MD5: 1c1348805d4f6f11311707b171f71350

Artifact 153: ☐ certificate-57.cer
Related to: stream 39

Src: network **Imports**: 0 **Type**: data
Size: 1350 **Exports**: 0 **AV Sigs**: 0
SHA256: 7f0085c2fe20d77f3882167dd5124e591469d43b3e15a9d6d686dbe6382dd901
MD5: 9afe4cccbdcb24e23401d406beaf3051

Artifact 154: ☐ certificate-119.cer
Related to: stream 74

Src: network **Imports**: 0 **Type**: data
Size: 1321 **Exports**: 0 **AV Sigs**: 0
SHA256: 8d45c7900387966bb4edbae21f740eeb29f10596dc130cd10afde8b075e4d991
MD5: 99105e8735abb40739b7be7e35e6ef8b

Artifact 155: ☐ Gartner.eot
Related to: stream 11

Src: network **Imports**: 0 **Type**: Embedded OpenType (EOT), Gartner family
Size: 67752 **Exports**: 0 **AV Sigs**: 0
SHA256: 00d6561e9feb9361b47a1e8bd3ca9e7d795d620124cc10791664959bd92eaee5
MD5: 52717cba0b135a970375983a9ec5bcbf

Artifact 156: ☐ imagehandler.ashx
Related to: stream 53

Src: network **Imports**: 0 **Type**: PNG - PNG image data, 200 x 74, 8-bit/color RGBA, non-int...
Size: 7502 **Exports**: 0 **AV Sigs**: 0
SHA256: 81278e76a448414c46166ad39d2df4e650472f76b4f94a178b28d2f3fdde39e8
MD5: 02038586cedbe9be7cfcf56d60867af9

Artifact 157: ☐ coupon_code1.js
Related to: stream 72

Src: network **Imports**: 0 **Type**: JS - ASCII text, with very long lines, with no line termi...
SHA256: ...bea0989e210a4fcb108862440ecfc2068675e4e028be60223242005d4c1c
Size: 1968 **Exports**: 0 **AV Sigs**: 0
MD5: f784887fc7a324d938310f731ed76ad1

Artifact 158: ☐ 3437.js
Related to: stream 75

Src: network **Imports**: 0 **Type**: JS - C source, ASCII text, with very long lines, with no ...
SHA256: ...7804a67570be2aad497a935514e039fb3a85cdbd360001ccd4553721eb5
Size: 11241 **Exports**: 0 **AV Sigs**: 0
MD5: 1e7efaae9fa37c3f7d5ae462c58a2a2a

Artifact 159: ☐ certificate-178.cer
Related to: stream 117

Src: network **Imports**: 0 **Type**: data
Size: 1205 **Exports**: 0 **AV Sigs**: 0
SHA256: 19400be5b7a31fb733917700789d2f0a2471c0c9d506c0e504c06c16d7cb17c0
MD5: aaee5cf8b0d8596d2e0cbe67421cf7db

Artifact 160: ☐ glyphicons-halflings-regular.eot
Related to: stream 9

Src: network **Imports**: 0 **Type**: HTML - HTML document, ASCII text
Size: 6096 **Exports**: 0 **AV Sigs**: 0
SHA256: c868e38088da2efe76aa6b0d37417156c5cd222fa227e2fb0a971540b5005bc0
MD5: 912447e2eec0b1c05d1b733b4ecfe7bc

Artifact 161: ☐ scholtz-tom.png;wa994f923ec35431f3
Related to: stream 43

Src: network **Imports**: 0 **Type**: PNG - PNG image data, 285 x 285, 8-bit/color RGBA, non-in...
Size: 11007 **Exports**: 0 **AV Sigs**: 0
SHA256: a1e806495d148bf31fd8d46efcf1307dd10410dbd267676e9b715718dc3b4967
MD5: 3d0cea0534eaf6d1f82a048e86981d87

Artifact 162: ☐ RobotoCondensed-Regular-webfont.eot Related to: stream 23

Src: networ**Imports**: 0 **Type**: Embedded OpenType (EOT), Roboto Co**SHA256**: family 6210b12b1324fcd446c75a016f4cf0448e53b7a4192b7141178faf14af4

Size: 21712 **Exports**: 0 **AV Sigs**: 0 **MD5**: 01a9358fc6594120b72d4d3c419dc356

Metadata | Behavioral Indicators | Network Activity | Processes | Artifacts | Registry Activity | File Activity

Src: networ**Imports**: 0 **Type**: GIF image data, version 89a, 1 x 1 **SHA256**: f1ccea6b7204d9f7913ab45e1afa51d79f83bd4f0319de937b0132e6e02b1aab

Size: 49 **Exports**: 0 **AV Sigs**: 0 **MD5**: dbefe00673f01d8b0f2791f3e30565cc

Artifact 164: ☐ imagehandler.ashx Related to: stream 50

Src: networ**Imports**: 0 **Type**: JPEG - JPEG image data, JFIF standard **SHA256**: resolution (D 4196cd5e40b30730ab1bb64eb08f9010c1032ff405ff99921f23bce

Size: 3593 **Exports**: 0 **AV Sigs**: 0 **MD5**: 8fefbff472d94e69d57b7026c74c82ff

Artifact 165: ☐ swg_cybersecurity_business_outcomes_h...g;wad8c6c964bb08c937 Related to: stream 105

Src: networ**Imports**: 0 **Type**: JPEG - JPEG image data, JFIF standard **SHA256**: aspect ratio, afb13753f6692a30c319c55db9caaa1eff7f5067339e9cd55fbaba56

Size: 27046 **Exports**: 0 **AV Sigs**: 0 **MD5**: ae82dd046f7d227c44a2bf10a3d5d9fe

Artifact 166: ☐ FaktConPro-Medium.eot Related to: stream 11

Src: networ**Imports**: 0 **Type**: Embedded OpenType (EOT), Fakt Con P **SHA256**: family c5fd6cd777dfb9f573584b97a8ac8188ceb29ded022321a882a6d66cba6a

Size: 20880 **Exports**: 0 **AV Sigs**: 0 **MD5**: 8418bb0ef68ec6e1b5ccc0465efbe120

Artifact 167: ☐ Roboto-Light-webfont.eot Related to: stream 11

Src: networ**Imports**: 0 **Type**: Embedded OpenType (EOT), Roboto Lig **SHA256**: 2517b97e2c0e1e6c8ceb9dd007015f897926bc504154137281eec4c1a9f9bdc9

Size: 20940 **Exports**: 0 **AV Sigs**: 0 **MD5**: a990f611f2305dc12965f186c2ef2690

Artifact 168: ☐ firstbrook-peter.png;waf9cc3d4152ec1525 Related to: stream 46

Src: networ**Imports**: 0 **Type**: PNG - PNG image data, 285 x 285, 8-bit/color RGBA, non-in... **SHA256**: 296599dc71b572f5dc6820bdd8c19356bdb705b2d981b628c361212949d5f944

Size: 14212 **Exports**: 0 **AV Sigs**: 0 **MD5**: be6e87eba48119846900e5ae25c8bfec

Artifact 169: ☐ er Related to: stream 6

Src: networ**Imports**: 0 **Type**: HTML - HTML document, ASCII text, wi **SHA256**: long lines, w 9b4facc04b7c38405a7d45772bd9b0d4a8b60dbb85a6964a69930

Size: 482 **Exports**: 0 **AV Sigs**: 0 **MD5**: 52af9ea8accb1a5d57c8776984dd172a

Artifact 170: ☐ imagehandler.ashx Related to: stream 52

Src: networ**Imports**: 0 **Type**: PNG - PNG image data, 200 x 80, 8-bit/color RGBA, non-int... **SHA256**: 9315aee0a2852ac41a2579d727d6e1d0893c0cf5a2bf3decbd16c47591a43ff3

Size: 7543 **Exports**: 0 **AV Sigs**: 0 **MD5**: ccfbb8be165c8b76f56b61c04f80da28

Artifact 171: ☐ summits_logo.png;wae1939c398a5538d1 Related to: stream 42

Src: networ**Imports**: 0 **Type**: PNG - PNG image data, 210 x 88, 8-bit/color RGBA, non-int... **SHA256**: 09d4527c1c5b55cd8462df81e803af368a82400fe08553f980d5fcafa0247e68

Size: 5931 **Exports**: 0 **AV Sigs**: 0 **MD5**: 11c39dd0c176f5250f4260bc31ca1d2f

Artifact 172: ☐ bootstrap-3.2.0.min.js;wa72cbcc36dacf519c Related to: stream 19

Src: networ**Imports**: 0 **Type**: ASCII text, with very long lines **SHA256**: 24cc29533598f962823c4229bc280487646a27a42a95257c31de1b9b18f3710f

Size: 31819 **Exports**: 0 **AV Sigs**: 0 **MD5**: abda843684d022f3bc22bc83927fe05f

Artifact 173: ☐ security-india Related to: stream 10

Src: networ**Imports**: 0