Flash Bulletin: Emotet Epoch 1 Changes its C2 Communication

cofense.com/flash-bulletin-emotet-epoch-1-changes-c2-communication/

Cofense March 15, 2019

We are currently noticing a change in the way that the Emotet botnet, specifically the epoch 1 variant, is communicating with the C2. In past versions, the client would typically perform a GET request with data contained in the cookie value. As of approximately 11pm UTC on March 14, this changed. The clients have begun to perform HTTP POSTs to what appear to be their C2s. The URI's contacted contain variable words in the paths. We are seeing form data passed with a name variable and data. This change will break researchers as well as certain detection technologies while they scurry to retool. We will continue to track this change and analyze what this means. Further details to come.

IOC's

Emotet E1 Client hash:
e0f04e2fbf3beed2dc836567006890f6f0442db78248cc2fd049437547be462e

Seen POST Uri's

178[.]78[.]64[.]80:8443/usbccid/
82[.]78[.]228[.]57:443/attrib/
82[.]78[.]228[.]57:443/taskbar/
139[.]59[.]19[.]157/acquire/results/
139[.]59[.]19[.]157/add/between/taskbar/merge/
139[.]59[.]19[.]157/attrib/img/report/
139[.]59[.]19[.]157/badge/sess/devices/enabled/
139[.]59[.]19[.]157/chunk/
139[.]59[.]19[.]157/codec/
139[.]59[.]19[.]157/devices/
139[.]59[.]19[.]157/free/add/report/merge/
139[.]59[.]19[.]157/glitch/
139[.]59[.]19[.]157/health/merge/
139[.]59[.]19[.]157/health/tlb/splash/
139[.]59[.]19[.]157/iab/report/between/merge/
139[.]59[.]19[.]157/jit/entries/enabled/
139[.]59[.]19[.]157/loadan/
139[.]59[.]19[.]157/loadan/child/odbc/
139[.]59[.]19[.]157/pdf/entries/entries/merge/
139[.]59[.]19[.]157/pnp/
139[.]59[.]19[.]157/prep/
139[.]59[.]19[.]157/prov/taskbar/entries/
139[.]59[.]19[.]157/prov/usbccid/
139[.]59[.]19[.]157/report/taskbar/
139[.]59[.]19[.]157/report/window/arizona/merge/
139[.]59[.]19[.]157/ringin/bml/health/
139[.]59[.]19[.]157/schema/iab/
139[.]59[.]19[.]157/scripts/usbccid/
139[.]59[.]19[.]157/sess/jit/usbccid/merge/
139[.]59[.]19[.]157/srvc/glitch/
139[.]59[.]19[.]157/srvc/pdf/
139[.]59[.]19[.]157/stubs/between/entries/merge/
139[.]59[.]19[.]157/teapot/arizona/splash/enabled/
139[.]59[.]19[.]157/tlb/srvc/schema/enabled/
139[.]59[.]19[.]157/usbccid/entries/site/
139[.]59[.]19[.]157/vermont/mult/
139[.]59[.]19[.]157/walk/between/
139[.]59[.]19[.]157/walk/enable/iplk/
139[.]59[.]19[.]157/walk/taskbar/
139[.]59[.]19[.]157/window/between/enabled/
152[.]171[.]65[.]137:8090/psec/rtm/vermont/enabled/
152[.]171[.]65[.]137:8090/splash/arizona/

165[.]227[.]213[.]173:8080/attrib/schema/vermont/enabled/
165[.]227[.]213[.]173:8080/ban/iab/
165[.]227[.]213[.]173:8080/ban/nsip/taskbar/
165[.]227[.]213[.]173:8080/bml/mult/prov/enabled/
165[.]227[.]213[.]173:8080/child/
165[.]227[.]213[.]173:8080/cookies/json/
165[.]227[.]213[.]173:8080/enabled/
165[.]227[.]213[.]173:8080/entries/srvc/
165[.]227[.]213[.]173:8080/loadan/loadan/
165[.]227[.]213[.]173:8080/prep/loadan/symbols/
165[.]227[.]213[.]173:8080/schema/iab/
165[.]227[.]213[.]173:8080/sess/
165[.]227[.]213[.]173:8080/site/bml/forced/merge/
165[.]227[.]213[.]173:8080/splash/enable/prov/enabled/
165[.]227[.]213[.]173:8080/sym/tpt/nsip/enabled/
165[.]227[.]213[.]173:8080/symbols/badge/
165[.]227[.]213[.]173:8080/tlb/nsip/
165[.]227[.]213[.]173:8080/usbccid/prov/sess/
173[.]248[.]147[.]186/attrib/usbccid/entries/
173[.]248[.]147[.]186/iab/odbc/forced/
173[.]248[.]147[.]186/mult/tlb/
173[.]248[.]147[.]186/mult/window/enabled/
173[.]248[.]147[.]186/pnp/taskbar/splash/
173[.]248[.]147[.]186/publish/
173[.]248[.]147[.]186/schema/mult/arizona/
173[.]248[.]147[.]186/teapot/acquire/
173[.]248[.]147[.]186/teapot/usbccid/
178[.]78[.]64[.]80:8443/acquire/entries/
178[.]78[.]64[.]80:8443/acquire/merge/forced/enabled/
178[.]78[.]64[.]80:8443/attrib/usbccid/
178[.]78[.]64[.]80:8443/devices/between/devices/enabled/
178[.]78[.]64[.]80:8443/devices/free/report/merge/
178[.]78[.]64[.]80:8443/devices/free/schema/enabled/
178[.]78[.]64[.]80:8443/json/sess/attrib/
178[.]78[.]64[.]80:8443/raster/
178[.]78[.]64[.]80:8443/tpt/
181[.]16[.]4[.]180/attrib/entries/report/
181[.]16[.]4[.]180/attrib/scripts/
181[.]16[.]4[.]180/between/scripts/child/enabled/
181[.]16[.]4[.]180/cookies/symbols/arizona/merge/
181[.]16[.]4[.]180/dma/
181[.]16[.]4[.]180/loadan/raster/

181[.]16[.]4[.]180/publish/child/tlb/merge/
181[.]16[.]4[.]180/raster/
181[.]16[.]4[.]180/window/tlb/symbols/enabled/
181[.]56[.]165[.]97:53/balloon/enabled/mult/
181[.]56[.]165[.]97:53/child/merge/chunk/enabled/
181[.]56[.]165[.]97:53/iplk/teapot/forced/
181[.]56[.]165[.]97:53/pdf/json/tlb/
181[.]61[.]221[.]146/chunk/iplk/
181[.]61[.]221[.]146/forced/attrib/enable/enabled/
186[.]137[.]133[.]132:8080/ringin/entries/
186[.]138[.]205[.]189/child/devices/add/enabled/
186[.]138[.]205[.]189/stubs/taskbar/
186[.]3[.]188[.]74/arizona/
186[.]3[.]188[.]74/cookies/scripts/arizona/
186[.]3[.]188[.]74/entries/
186[.]3[.]188[.]74/json/health/odbc/
186[.]3[.]188[.]74/prep/window/
186[.]3[.]188[.]74/results/attrib/
186[.]3[.]188[.]74/schema/badge/
186[.]3[.]188[.]74/srvc/report/forced/enabled/
186[.]3[.]188[.]74/stubs/scripts/vermont/enabled/
189[.]208[.]239[.]98:443/enable/raster/prep/
189[.]208[.]239[.]98:443/pdf/cookies/
189[.]208[.]239[.]98:443/scripts/entries/mult/enabled/
190[.]117[.]206[.]153:443/attrib/loadan/
190[.]117[.]206[.]153:443/badge/ban/vermont/
190[.]117[.]206[.]153:443/devices/
190[.]117[.]206[.]153:443/iplk/pnp/
190[.]117[.]206[.]153:443/merge/window/
190[.]117[.]206[.]153:443/publish/
190[.]117[.]206[.]153:443/ringin/odbc/
190[.]117[.]206[.]153:443/sess/balloon/glitch/
190[.]117[.]206[.]153:443/symbols/
190[.]146[.]86[.]180:443/child/odbc/forced/enabled/
190[.]146[.]86[.]180:443/enabled/devices/enabled/merge/
190[.]146[.]86[.]180:443/guids/between/devices/
190[.]146[.]86[.]180:443/guids/site/splash/enabled/
190[.]146[.]86[.]180:443/merge/balloon/
190[.]146[.]86[.]180:443/mult/badge/glitch/merge/
190[.]146[.]86[.]180:443/pnp/
190[.]146[.]86[.]180:443/raster/badge/odbc/enabled/
190[.]146[.]86[.]180:443/srvc/json/

190[.]15[.]198[.]47/arizona/pnp/
190[.]15[.]198[.]47/balloon/cookies/devices/enabled/
190[.]15[.]198[.]47/cab/sess/
190[.]15[.]198[.]47/guids/acquire/splash/
190[.]15[.]198[.]47/img/balloon/
190[.]15[.]198[.]47/schema/report/vermont/enabled/
190[.]15[.]198[.]47/scripts/
190[.]15[.]198[.]47/site/enabled/
190[.]15[.]198[.]47/vermont/
192[.]155[.]90[.]90:7080/acquire/
192[.]155[.]90[.]90:7080/free/prov/chunk/
192[.]155[.]90[.]90:7080/prep/stubs/
192[.]163[.]199[.]254:8080/add/enable/symbols/enabled/
192[.]163[.]199[.]254:8080/balloon/balloon/
192[.]163[.]199[.]254:8080/report/
192[.]163[.]199[.]254:8080/report/acquire/schema/enabled/
192[.]163[.]199[.]254:8080/rtm/srvc/
192[.]163[.]199[.]254:8080/scripts/health/results/
208[.]180[.]246[.]147/add/forced/mult/enabled/
208[.]180[.]246[.]147/tlb/window/
208[.]180[.]246[.]147/usbccid/results/chunk/enabled/
23[.]254[.]203[.]51:8080/acquire/scripts/iab/enabled/
23[.]254[.]203[.]51:8080/arizona/ban/symbols/
23[.]254[.]203[.]51:8080/forced/merge/enable/enabled/
23[.]254[.]203[.]51:8080/json/
5[.]9[.]128[.]163:8080/devices/tpt/
5[.]9[.]128[.]163:8080/enable/sess/tlb/merge/
5[.]9[.]128[.]163:8080/odbc/odbc/enable/enabled/
50[.]246[.]45[.]249:7080/cookies/rtm/
50[.]246[.]45[.]249:7080/dma/cookies/
50[.]246[.]45[.]249:7080/loadan/codec/
51[.]255[.]50[.]164:8080/arizona/srvc/
51[.]255[.]50[.]164:8080/attrib/schema/results/enabled/
51[.]255[.]50[.]164:8080/ban/symbols/acquire/merge/
51[.]255[.]50[.]164:8080/enabled/
51[.]255[.]50[.]164:8080/iab/prep/scripts/
51[.]255[.]50[.]164:8080/iplk/
51[.]255[.]50[.]164:8080/loadan/
51[.]255[.]50[.]164:8080/pdf/psec/schema/
51[.]255[.]50[.]164:8080/publish/
51[.]255[.]50[.]164:8080/site/xian/
51[.]255[.]50[.]164:8080/splash/symbols/acquire/merge/

51[.]255[.]50[.]164:8080/srvc/publish/forced/
51[.]255[.]50[.]164:8080/taskbar/scripts/json/
51[.]255[.]50[.]164:8080/walk/tlb/raster/merge/
51[.]255[.]50[.]164:8080/window/
66[.]209[.]69[.]165:443/between/symbols/
66[.]209[.]69[.]165:443/enabled/walk/
66[.]209[.]69[.]165:443/prep/cone/enable/enabled/
69[.]163[.]33[.]82:8080/add/psec/
69[.]163[.]33[.]82:8080/cookies/splash/chunk/enabled/
69[.]163[.]33[.]82:8080/loadan/badge/publish/enabled/
69[.]163[.]33[.]82:8080/sess/vermont/
69[.]163[.]33[.]82:8080/srvc/
70[.]28[.]22[.]105:8090/arizona/
70[.]28[.]22[.]105:8090/report/tpt/chunk/
70[.]28[.]22[.]105:8090/stubs/balloon/enable/
72[.]47[.]248[.]48:8080/balloon/report/iab/
72[.]47[.]248[.]48:8080/img/raster/arizona/
72[.]47[.]248[.]48:8080/results/merge/symbols/
72[.]47[.]248[.]48:8080/vermont/results/
82[.]78[.]228[.]57:443/acquire/
82[.]78[.]228[.]57:443/arizona/nsip/balloon/
82[.]78[.]228[.]57:443/badge/cookies/teapot/enabled/
82[.]78[.]228[.]57:443/balloon/
82[.]78[.]228[.]57:443/ban/
82[.]78[.]228[.]57:443/between/
82[.]78[.]228[.]57:443/child/usbccid/loadan/
82[.]78[.]228[.]57:443/chunk/health/forced/
82[.]78[.]228[.]57:443/codec/
82[.]78[.]228[.]57:443/devices/
82[.]78[.]228[.]57:443/devices/vermont/
82[.]78[.]228[.]57:443/dma/ringin/enabled/
82[.]78[.]228[.]57:443/enable/entries/
82[.]78[.]228[.]57:443/enabled/child/json/
82[.]78[.]228[.]57:443/glitch/
82[.]78[.]228[.]57:443/iab/scripts/add/enabled/
82[.]78[.]228[.]57:443/mult/publish/sym/
82[.]78[.]228[.]57:443/pdf/arizona/balloon/
82[.]78[.]228[.]57:443/pdf/site/
82[.]78[.]228[.]57:443/prov/enable/splash/enabled/
82[.]78[.]228[.]57:443/schema/publish/vermont/
82[.]78[.]228[.]57:443/site/entries/
82[.]78[.]228[.]57:443/site/glitch/

> 82[.]78[.]228[.]57:443/stubs/ban/ban/merge/
> 82[.]78[.]228[.]57:443/taskbar/entries/
> 82[.]78[.]228[.]57:443/tlb/
> 82[.]78[.]228[.]57:443/tpt/arizona/child/merge/
> 82[.]78[.]228[.]57:443/walk/
> 82[.]78[.]228[.]57:443/xian/

Don't miss out on any of our phishing updates! Subscribe to our blog.