랜섬프리에 의한 CryptXXX 3.0 차단 분석

차단일시 : 2016년 6월 16일 10:57:46~49초

CryptXXX : 2016년 4월 중순경부터 유포되기 시작, 5월초에 2.0, 5월 중순경에 3.0 출현

공격 프로세스 : C:₩Users₩optiplex780(로그인 계정)₩AppData₩Local₩Temp₩explorer.exe

프로세스를 윈도우 시스템 프로세스인 explorer로 위장하였으나, 랜섬프리가 추적한 path를 보면 오리지널 explorer 위치가 아님을 알 수 있습니다.

```
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
C:₩Users₩optiplex780₩AppData₩Local₩Temp₩explorer.exe
```

랜섬프리가 방어한 파일

```
C:₩Users₩optiplex780₩Documents₩NeoiCube₩PMX0210__flex_20141001111421.xls, 609380, , 0,
C:₩Users₩optiplex780₩Documents₩NeoiCube₩PMX0210__flex_20150303114857.xls, 29686, , 0,
C:₩Users₩optiplex780₩Documents₩NeoiCube₩PMX0210__flex_20150303114928.xls, 196750, , 0,
C:₩Users₩optiplex780₩Documents₩NeoiCube₩PMX0210__flex_20150319090423.xls, 21059, , 0,
C:₩Users₩optiplex780₩Documents₩NeoiCube₩PMX0210__flex_20150319090433.xls, 134701, , 0,
C:₩Users₩optiplex780₩Documents₩NeoiCube₩PMX0210__flex_20150610144637.xls, 62589, , 0,
C:₩Users₩optiplex780₩Documents₩NeoiCube₩PMX0210__flex_20150610144643.xls, 440129, , 0,
C:₩Users₩optiplex780₩Documents₩NeoiCube₩PMX0210__flex_20150610144655.xls, 463753, , 0,
C:₩Users₩optiplex780₩Documents₩NeoiCube₩PMX0210__flex_20150702163352.xls, 246623, , 0,
C:₩Users₩optiplex780₩Documents₩NeoiCube₩PMX0210__flex_20150702163604.xls, 259151, , 0,
C:₩Users₩optiplex780₩Documents₩NeoiCube₩PMX0210__flex_20150702163618.xls, 246623, , 0,
C:₩Users₩optiplex780₩Documents₩NeoiCube₩PMX0210__flex_20160303110644.xls, 29026, , 0,
C:₩Users₩optiplex780₩Documents₩NeoiCube₩PMX0210__flex_20160303110719.xls, 187014, , 0,
C:₩Users₩optiplex780₩Documents₩NeoiCube₩PMX0210__flex_20160310164244.xls, 134762, , 0,
C:₩Users₩optiplex780₩Documents₩NeoiCube₩PMX0210__flex_20160407172301.xls, 38866, , 0,
C:₩Users₩optiplex780₩Documents₩NeoiCube₩PMX0210__flex_20160407172322.xls, 253427, , 0,
C:₩Users₩optiplex780₩Documents₩NeoiCube₩SYB0010__flexH_20150122122914.xls, 3584, , 0,
C:₩Users₩optiplex780₩Documents₩NeoiCube₩SYB0010__flexH_20151203114427.xls, 93507, , 0,
C:₩Users₩optiplex780₩Documents₩NeoiCube₩SYC0320__flexH_20140812162217.xls, 6144, , 0,
C:₩Users₩optiplex780₩Documents₩NeoiCube₩SYC0320__flexH_20150717141823.xls, 6144, , 0,
C:₩Users₩optiplex780₩Documents₩rexpe.pdf, 300281, , 0,
C:₩Users₩optiplex780₩Documents₩rexpert.pdf, 302173, , 0,
C:₩Users₩optiplex780₩Documents₩rexpert3.pdf, 302556, , 0,
C:₩Users₩optiplex780₩Documents₩발주하기.ppt, 103936, , 0,
C:₩Users₩optiplex780₩Documents₩ㅡㅡㅡ 15년 12월_구매개발팀 원가절감 계획대비 실적.xlsx, 100147
C:₩Users₩optiplex780₩Documents₩지텍 입고 리스트 20160318.ppt, 101376, , 0,
C:₩Users₩optiplex780₩Documents₩카카오톡 받은 파일₩(Final)160406 CYM-CYMAI DIE & TOOLS 04월 7일
C:₩Users₩optiplex780₩Documents₩카카오톡 받은 파일₩160303 ETR-CYMAI Carbon sheet & tools 03월 4
C:₩Users₩optiplex780₩Documents₩카카오톡 받은 파일₩160309 CYM-CYMAI D,CONE & Part for 45ton tri
C:₩Users₩optiplex780₩Documents₩카카오톡 받은 파일₩160329 ETR-CYMAI Tools 03월 31일 선적건.xlsx
C:₩Users₩optiplex780₩Documents₩카카오톡 받은 파일₩160330 CYM-CYMAI DIE & TOOLS 03월 31일 선적건
C:₩Users₩optiplex780₩Documents₩카카오톡 받은 파일₩7속 DCT_QCY_출고LIST.xlsx, 647647, , 0,
C:₩Users₩optiplex780₩Documents₩카카오톡 받은 파일₩쿠론사판.pdf, 6056682, , 0,
C:₩Users₩optiplex780₩Downloads₩Trimming machine.xlsx, 194824, , 0,
C:₩Users₩optiplex780₩Downloads₩에쓰오일토탈-협력업체 매뉴얼.pptx, 81, , 0,
C:₩Users₩optiplex780₩거래명세서 -ㅡ ㅡ ㅡ .xlsx, 30823, , 0,
```