

侵入の痕跡 (IoC : Indicators of Compromise)

ハッシュ値

ハッシュ値	検出名	内容
dffa99b9fe6e7d3e19asfba38c9f7ec739581f656	Ransom.Linux.TARGETCOMP.YXEEQT	TargetCompany の Linux 型亜種
2b82b463dab61cd3d7765492d7b4a529b4618e57	Trojan.SH.TARGETCOMP.THEAGBD	シェルスクリプト
9779aa8eb4c6f9eb809ebf4646867b0ed38c97e1	Ransom.Win64.TARGETCOMP.YXECMT	アフィリエイト「vampire」に関連する TargetCompany のファイル
3642996044cd85381b19f28a9ab6763e2bab653c	Ransom.Win64.TARGETCOMP.YXECFT	アフィリエイト「vampire」に関連する TargetCompany のファイル
4cdee339e038f5fc32dde8432dc3630afd4df8a2	Ransom.Win32.TARGETCOMP.SMYXCLAZ	アフィリエイト「vampire」に関連する TargetCompany のファイル
0f6bea3ff11bb56c2daf4c5f5c5b2f1afd3d5098	Ransom.Win32.TARGETCOMP.SMYXCLAZ	アフィリエイト「vampire」に関連する TargetCompany のファイル

URL

URL	検出名	内容
hxxp://111.10.231[.]151:8168/general/vmeett/upload/temp/x.sh	90 – Untested	スクリプトのダウンロード URL
hxxp://111.10.231[.]151:8168/general/vmeett/upload/temp/x	79 – Disease Vector	ランサムウェア用ペイロードのダウンロード URL
hxxp://111.10.231[.]151:8168/general/vmeett/upload/temp/post.php	79 – Disease Vector	アップロード URL