Lockbit 2.0 ランサムウェア急上昇
March 08, 2022 年 3 月 8 日 Minerva のブログから

LockBit 2.0 の Onion ウエブサイトによると、このグループは既に 100 社を超える企業組織に対し攻撃を実現しました。

Lockbit とは?
Lockbit グループはランサムウェアアズアサービス（RaaS）でマルウェアの開発やダークウェブ上でマルウェアの闇取引をしています。ランサムウェアを各ハッキンググループまたは個人などへ拡散することにより、多くの感染を広げることに成功しています。

LockBit 2.0 グループは 2020 年の初期にアフィリエイトプログラムを展開しました。昨年の夏には新種のペイロードを追加し、マルウェアが高度化しています。最も大きな変化としては、二重の脅迫機能を実装することにより、多くの企業組織に対し更なる脅威を与えてきています。

最新の FBI が最近リリースしているレポートでは、攻撃を絞った組織に対し、内通者を探し出し攻撃を仕掛けるような手法を行い、攻撃に成功した暁には内通者に報酬を約束しているようです。

Lockbit の現在
LockBit2.0 は攻撃を絞った相手に対し、StealBit、Cobalt Strike 及び Metasploit など、複合攻撃手法でデータを窃取し、ランサムの支払いを拒否すると、データを公開すると脅します。

LockBit 2.0 は的を絞ったターゲットのネットワーク侵入及びファイル窃取を実現するために協力者（共謀者）を募って攻撃を実施します。協力者はフィッシング攻撃、脆弱性のアプリ又はRDP（リモートデスクトップ）アカウントへブルートフォース攻撃などのマルウェアを利用し初期攻撃を開始します。

Lockbit の検知回避手法

LockBit グループはセキュリティ製品に検知と分析から免れるためにいくつかの回避手法を用います。以下は回避手法です。

1. バイナリー難読化
2. FNV ハッシュアルゴリズムを使用する API 暗号化とダイナミック解決
3. デバッガースレッドから隠蔽されている複合スレッドの実行

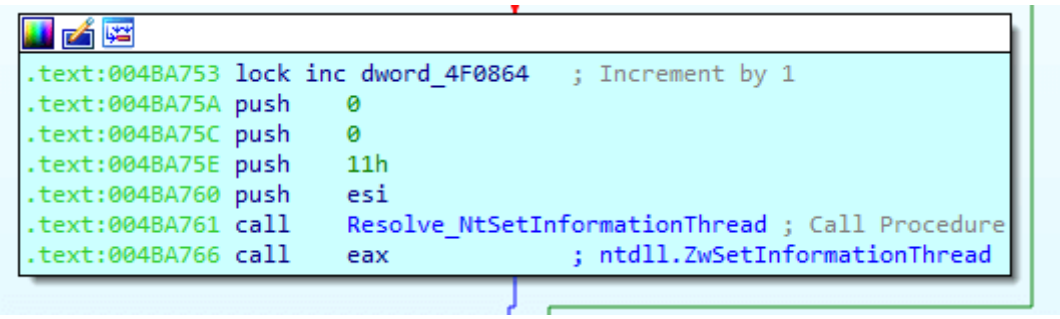

図 1 - 隠されたスレッド生成

システム侵入に成功すると、LockBit はネットワーク構造を認識するためにスキャナーを使用し、攻撃目標のドメインコントローラーを探します。また複数のバッチファイルを使用し、プロセス、サービスやセキュリティツールを無効化してしまいます。

```
aWxserver db 'wxServer',0
aWxserverviewSq db 'wxServerView,sqlmangr,RAgui,supervise,Culture,Defwatch,winword,QB'
db 'W32,QBDBMgr,qbupdate,axlbridge,httpd,fdlauncher,MsDtSrvr,java,360'
db 'se,360doctor,wdswfsafe,fdhost,GDscan,ZhuDongFangYu,QBDBMgrN,mysql'
db 'd,AutodeskDesktopApp,acwebbrowser,Creative Cloud,Adobe Desktop Se'
db 'rvice,CoreSync,Adobe CEF,Helper,node,AdobeIPCBroker,sync-taskbar,'
db 'sync-worker,InputPersonalization,AdobeCollabSync,BrCtrlCntr,BrCcU'
db 'xSys,SimplyConnectionManager,Simply.SystemTrayIcon,fbguard,fbserv'
db 'er,ONENOTEM,wsa_service,koaly-exp-engine-service,TeamViewer_Servi'
db 'ce,TeamViewer,tv_w32,tv_x64,TitanV,Ssms,notepad,RdrCEF,sam,oracle'
db ',ocssd,dbsnmp,synctime,agntsvc,isqlplussvc,xfssvccon,mydesktopser'
db 'vice,ocautoupds,encsvc,tbirdconfig,mydesktopqos,ocomm,dbeng50,sqb'
db 'coreservice,excel,infopath,msaccess,mspub,onenote,outlook,powerpn'
db 't,steam,thebat,thunderbird,visio,wordpad,bedbh,vxmon,benetns,beng'
db 'ien,pvlsvr,beserver,raw_agent_svc,vsnapvss,CagService,DellSystemD'
db 'etect,EnterpriseClient,ProcessHacker,Procexp64,Procexp,GlassWire,'
db 'GWCtlSrv,WireShark,dumpcap,j0gnjko1,Autoruns,Autoruns64,Autoruns6'
db '4a,Autorunsc,Autorunsc64,Autorunsc64a,Sysmon,Sysmon64,procexp64a,'
db 'procmon,procmon64,procmon64a,ADExplorer,ADExplorer64,ADExplorer64'
db 'a,tcpview,tcpview64,tcpview64a,avz,tdsskiller,RaccineElevatedCfg,'
db 'RaccineSettings,Raccine_x86,Raccine,Sqlservr,RTVscan,sqlbrowser,t'
db 'omcat6,QBIDPService,notepad++,SystemExplorer,SystemExplorerServic'
db 'e,SystemExplorerService64,Totalcmd,Totalcmd64,VeeamDeploymentSvc',0
```

図 2 - LockBit に終了させられた復号プロセスリスト

```
aWrapperDefwatc db 'wrapper,DefWatch,ccEvtMgr,ccSetMgr,SavRoam,Sqlservr,sqlagent,sqla'
db 'dhlp,Culserver,RTVscan,sqlbrowser,SQLADHLP,QBIDPService,Intuit.Qu'
db 'ickBooks.FCS,QBCFMonitorService, msmdsrv,tomcat6,zhudongfangyu,vm'
db 'ware-usbarbitator64,vmware-converter,dbsrv12,dbeng8,MSSQL$MICROSO'
db 'FT##WID,MSSQL$VEEAMSQL2012,SQLAgent$VEEAMSQL2012,SQLBrowser,SQLWr'
db 'iter,FishbowlMySQL,MSSQL$MICROSOFT##WID,MySQL57,MSSQL$KAV_CS_ADMI'
db 'N_KIT,MSSQLServerADHelper100,SQLAgent$KAV_CS_ADMIN_KIT,msftesql-E'
db 'xchange,MSSQL$MICROSOFT##SSEE,MSSQL$SBSMONITORING,MSSQL$SHAREPOIN'
db 'T,MSSQLFDLauncher$SBSMONITORING,MSSQLFDLauncher$SHAREPOINT,SQLAge'
db 'nt$SBSMONITORING,SQLAgent$SHAREPOINT,QBFCService,QBVSS,YooBackup,'
db 'YooIT,vss,sql,svc$,MSSQL,MSSQL$,memtas,mepocs,sophos,veeam,backup'
db ',bedbg,PDVFSService,BackupExecVSSProvider,BackupExecAgentAccelera'
db 'tor,BackupExecAgentBrowser,BackupExecDiveciMediaService,BackupExe'
db 'cJobEngine,BackupExecManagementService,BackupExecRPCService,MVArm'
db 'or,MVarmor64,stc_raw_agent,VSNAPVSS,VeeamTransportSvc,VeeamDeploy'
db 'mentService,VeeamNFSSvc,AcronisAgent,ARSM,AcrSch2Svc,CASAD2DWebSv'
db 'c,CAARCUpdateSvc,WSBExchange,MSExchange,MSExchange$',0
```

図 3 - LockBit に終了させられた復号サービスリスト

彼らは侵入したデバイスのホスト名、ホスト設定、ドメイン情報、ローカルドライブ設定、リモート共有や外付けストレージデバイスなどを特定し情報収集します。最終的にシャドウコピーも削除し、自給自足型攻撃手法を用いて攻撃の足掛かりを作ります。 他のロシアベースのランサムウェアオペレーションとは異なり、LockBit 2.0 はシステムとユーザ言語を決定し、攻撃対象が東欧諸国の 13 言語の一つに該当すると攻撃対象外と設定しているようです。

2021 年 10 月以降は、このグループは Linux ホストである ESXi サーバへ攻撃を伸ばしてきています。

Minerva は Lockbit 2.0 から先制防御

Minerva のエンドポイントセキュリティーはLockbitのマルウェアが検知回避を試みても、マルウェアの実行を阻止します。Lockbit は数々の回避テクニックで通常のセキュリティ製品では素通されてしまうことがありますが、Minerva はマルウェア行動する前に阻止します。

Minerva 製品（Minerva Armor）についてのお問い合わせは Pico Technologies（info@pico-t.co.jp）までお願い致します。