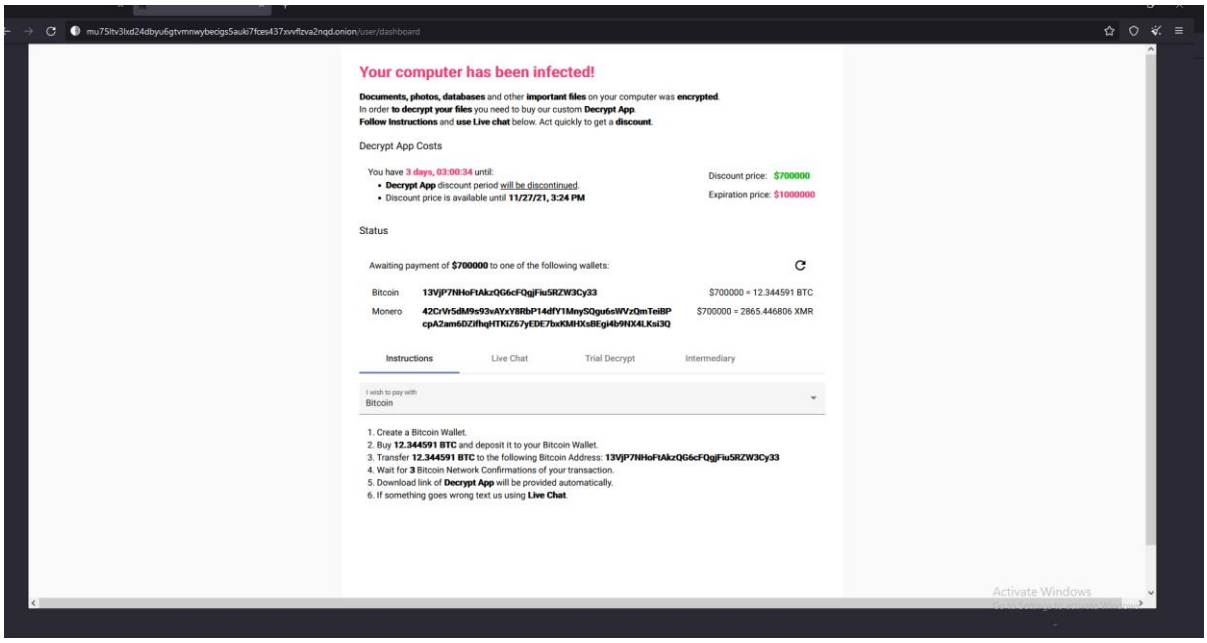
Minerva Labs 社インシデントチームが顧客のネットワークをランサムウェア攻撃から防御
2021 年 11 月 24 日 Minerva のブログから

今週の初めに起こったことですが、弊社の顧客からインシデントレスポンスチームへ緊急のリクエストがあり、彼らの新規カスタマーが、ランサム攻撃を受けたので調査してほしいとのリクエストがありました。



Minerva インシデントチームが早急に介入し、カスタマーエンドポイントに Minerva Armor エージェントをインストールして観察することにしました。

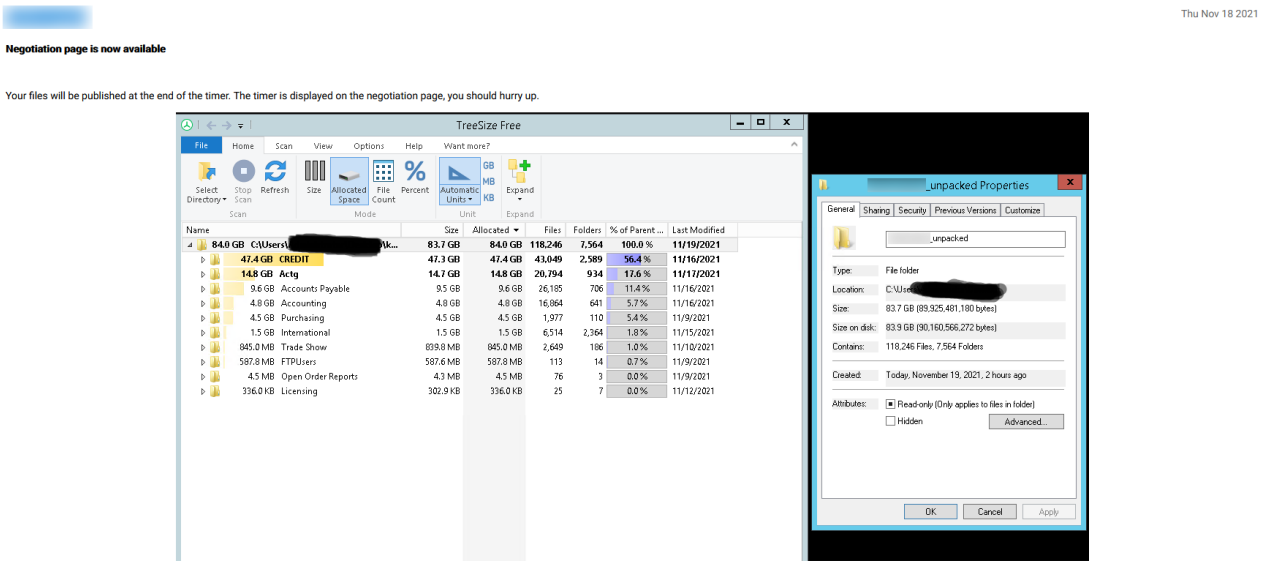
Minerva 製品は、マルウェアが攻撃を実行する前に先制防御するソリューションですが、今回のケースでは、初期の攻撃でもありピンポイント感染で済み、ネットワーク全体の防御を復帰し、危機一髪でランサムウェア攻撃の蔓延を防ぐことができました。インシデント調査後、このランサムウエアについて興味深い発見もありました。

The Rust Ransomware

このランサムウェアは Rust プログラム言語で書かれており、以下の [github]から同類のマルウェアを参照することができます。

このランサムウェアは 2021 年 11 月 18 日に確認され（今回のインシデントが起こる 4 日前）、この時点で、ほとんどのアンチウィルスソフトベンダーでは検知できない未知のマルウェアでした（VirusTotal で 67 社の内 5 社が認知）。

攻撃者はどうやら長い間被害者のエンドポイントへ潜んでおり、EPP 又は EDR ソリューションに検知されることなく管理者の認証情報などを不正取得しているようでした。それから 84GB のデータを抽出し、ファイルをダウンロードする事で.sykffle 拡張子を使用して暗号化されました。



ランサムウェア攻撃を受けて Winword, Browser や Onenote などがシャットダウンされ、これらのファイルが開いている状態では、暗号化されてしまいます。その上にデータを回復する為のツールも削除され四方八方からなす術もなく塞がれてしまう状況に陥ります。

残念なことですが、今回のケースは被害者のセキュリティー上に今後も影響を及ぼすこともあり（各マルウェアサンプルはカスタムビルド仕様で攻撃手法がユニーク）、一般に IOC（セキュリティ侵害インジケーター）を公表することはできません。

Minerva Armor を事前にインストールしておいたら、このような攻撃を受けずに済んだと思います。

どうやってランサムウェア攻撃から防ぐことができるのか？

各種ランサムウェアはそれぞれ異なる攻撃手法で攻撃を仕掛けてきます。いくつかのマルウェアでは高度なエクスプロイトが OS 上の脆弱性を突き侵入されてしまいますが、多くのケースではユーザーがフィッシング攻撃手法などで攻撃者に攻撃のチャンスを与えてしまうことです。

あらゆるランサムウェア攻撃から検知及び攻撃を防ぐシンプルな方法はないということです。だからこそ攻撃手法の調査及び今後の防御対策 — すなわち未知のランサムウェア攻撃で一般に知られていないマルウェアを防御することが必須課題になります。

Minerva は、サイバーセキュリティのエキスパートが集結し、未知のマルウェアから先制防御するテクノロジーであなたの企業組織からサイバー攻撃をシャットアウトします。

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。