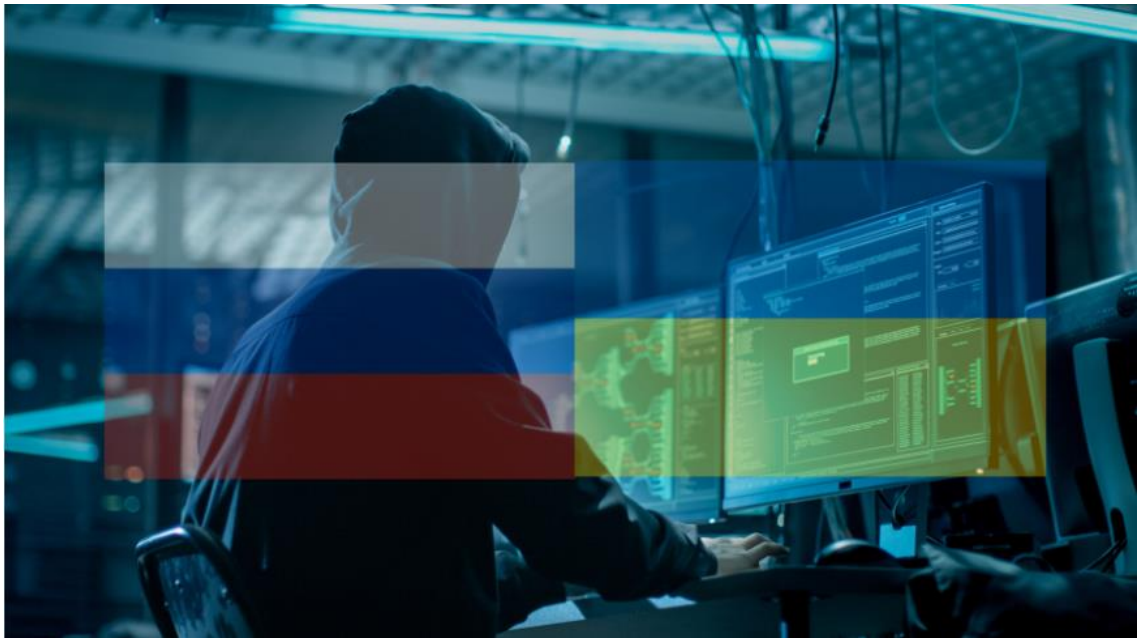

ウクライナネットワークがワイパー(Wiper)マルウェアの攻撃を受ける
2022 年 2 月 24 日 Minerva のブログから

ロシアはウクライナに対し、サイバー攻撃を仕掛け始めました。ワイパーマルウェア攻撃の波が押し寄せ、ウクライナのネットワーク上の重要ファイルを破壊しようとしています。

ランサムウェアや他のタイプのマルウェアのような身代金の獲得を目的とする攻撃ではなく、ワイパーマルウェアは単に攻撃ターゲットに対しデータを破壊し消去しようとする目的です。この特殊な攻撃はファイルを破壊だけでなく、ハードドライブのマスターブートレコード(MBR)を破壊することであり、これを破壊されると甚大なダメージとなります。この精巧な攻撃手法は、攻撃開始前のある期間内に足掛かりを作り水平攻撃を展開するようです。

攻撃は最終ステージに実行

攻撃実行ステージは最終ステージに行われます。最大の攻撃効果を得るためにマルウェアはネットワーク内で攻撃の足掛かりを構築した後に実行されるということです。

その攻撃の足掛かりを作るために、できるだけネットワーク侵入時に検知されないことが重要です。ある一定期間潜伏しながら攻撃の準備を着々と進め、最大の被害を被らせることです。数多くの検知回避テクニックを繰り返し行い、侵入に築かれずにネットワーク内に存在し続けるのです。

マルウェアが足掛かりを完成すると今まで静寂であったC&Cサーバから攻撃を実行するコマンドが伝達されます。今回のケースでは、ロシアのハッカーがウクライナの多くのネットワーク内に侵入した後、コマンドサーバーからの攻撃合図を待ち構えているのです。

ワイパーマルウェア感染は ESET と Symantec で検知されており、初期のワイパー攻撃は 2022 年 2 月 23 日 14 時 52 分(ウクライナ現地時間)頃と当日の夕方 5 時過ぎに ESET で検知記録されました。ESET はこのマルウェアを KillDisk.NCV.と呼称しています。その間 Symantec のツイッターでは、新規のマルウェアハッシュを共有しました。

ハッシュは以下の通りです。
1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591, in a tweet.

マルウェアハッシュは、特定のマルウェアを特定するために使用され、最終的にハッシュ化されますが、このマルウェアはコード再編集などを行うツールを使用し、マルウェアのバイナリーコードを変更することができます。よって類似する亜種的なマルウェアとして本来の悪意機能を温存させることができてしまいます。このことからシグネチャーベースのセキュリティ製品ではこのマルウェアを検知することは困難と言えます。

このマルウェアの攻撃先はほとんどがウクライナの金融機関と政府系のコントラクターですが似たような攻撃がラトビアとリトアニアでも確認されており、このことから 2017 年の NotPetya マルウェア攻撃を思い起こさせます。NotPetya 攻撃は従来ウクライナに対し攻撃を開始していたのですが、近隣諸国へも足を広げ最終的には世界中に蔓延しました。この攻

撃の結果、約 100 億ドルのダメージを与えたという事です。
（New Petya ランサムウェア攻撃を防御、2017 年 6 月 27 日 Minerva のブログもご覧ください。）

EST のテクニカル分析によると KillDisk.NCV.は正当なディスクパティションツールである EaseUS Partition Master を利用しているようです。この機能を利用してファイルを破壊し、強制的にリブートしてシステムを破壊します。しかしながらこのワイパーマルウェアは MBR も破壊するので、デバイスは OS 上でリブートできなくなり、デバイス自体を不可にしてしまいます。ワイパー攻撃は DDos 攻撃から始まり、ネットワーク通信に打撃を与えます。

Whispergate と類似

このワイパーマルウェアは WhisperGate マルウェアと似ており、今年早々にウクライナのシステムが感染しました。KillDisk.NCV,のように WhisperGate は MBR を破壊し、ランサムウェアを併発させました。

これらのサイバー攻撃の国籍は不明のままですが、このサイバー攻撃のターゲット地域などの事実を集めることにより、ロシアのハッカーが関与していることが疑われます。政府主導でこの攻撃を防御するために、事前に自国の重要ファイルが消去されたり、IT システムインフラが破壊される前にセキュリティ強化対処が早急な課題となるでしょう。

政府だけで解決は困難

米国では、サイバーセキュリティ・インフラセキュリティ庁（CISA）がこの攻撃をロシア政府がスポンサーであると認定し、主要なインフラに脅威を与え、全組織に対し最重要のサイバーアラートを発しています。政府のガイダンスとして Shields Up Guidance を発行しており、早急な対策をとるように促しています。

地政学的な緊張が高まり、サイバー攻撃が発生し始め、サイバーインフラが脆弱である組織は恰好のターゲットにされてしまうでしょう。よって組織はセキュリティ強化と対策が必須課題となります。

Minerva はこのようなタイプの攻撃からどのように先制防御できるのか。

このブログの最初でお話ししましたように攻撃が効果的に奏するには組織ネットワークに侵入後、攻撃の足掛かりを構築する事なのです。またマルウェア自体がアラート検知されないことが必須となります。このマルウェアは多様な検知回避を利用して存在しようと試みますが、Minerva 製品はこれらのマルウェアの実行活動をシャットダウンさせることで先制防御を行います。Minerva の強い点は、ネットワークへ不正侵入を試み、検知回避テクニックを駆使する未知のマルウェアに対し、徹底的に先制防御を行うエンドポイントセキュリティ製品です。

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。