マルウェア検知回避手法―自給自足型マルウェア
2022 年 3 月 14 日 Minerva のブログから

今回のブログはマルウェア開発者がセキュリティ製品から検知回避するテクニックについて、お話ししたいと思います。前回はサンドボックス検知回避についての詳細をお話致しました。

サンドボックス検知回避のブログでは、昨今のマルウェアはターゲットのネットワークへ侵入後、直ちに攻撃を仕掛けてデータを破壊したりなどはせず、セキュリティツールなどに検知されないように幾つもの回避手法で攻撃の足掛かりを築いていきます。

さて今回のブログでは自給自足型（LotL）攻撃の検知回避についてお話ししたいと思います。

自給自足型（LotL）とは？
自給自足型（LotL）攻撃は OS に装備されているビルトインシステム、ライブラリー、ツールなどネイティブツール利用して検知を回避する手法の一つです。OS に内蔵している機能やツールは元々正当である故に、悪用されて稼働されているとしてもセキュリティ製品の分析ツールでは特に問題なしと判定してしまうでしょう。

これらの正当なツールを利用して仕掛ける攻撃を自給自足型と言われていて、LOLbinaries 又は LOLbin と呼称されています。LOLbins で最も悪用されるツールを幾つか挙げますと Powershell, rundll.exe, regsvr32.exe, certutil.exe, wmin.exe, schtasks.exe などです。

よってマルウェアが LOLbins を悪用して仮想環境又はサンドボックス環境に見せかけたり、水平攻撃や悪意のあるアーティファクトをダウンロードしたり、データ窃取や更なる攻撃準備へ展開しても問題のない OS オペレーションとして認識されてしまいアラートが発せられません。

LotL は許可リスト、ホワイトリストなどのアプリケーションについても攻撃目的で利用します。LotL 特性のマルウェアはデジタル署名などのソフトウエアなどが信頼されていないなど勝手に許可リストなどをコントロールすることが可能です。

それでは次に LOLbins がどのように悪意のあるプロセスを実行し、検知されるのを回避するのかいくつかの例を見ていきましょう。

WMI を悪用して検知回避

WMI は Windows Management Instrumentation の略式ですが、この機能は Windows を一括統括する機能を持ち合わせており、最近のバージョンではプリインストールされています。OS のセキュリティ設定、システム特性の設定、スケジュールタスクプロセスなど多くのマネージメント機能を管理する重要なツールです。マルウェアはこの機能を悪用することにより、甚大なダメージを与える可能性を占めています。

WMI はラニングプロセス、レジストリーキー、インストールサービスなど WMI のマネージメントに属する重要な機能があります。どれだけクリティカルなのか例を挙げますと、マルウェアは root¥SecurityCenter2 namespace へクエリーを発信することにより、Windows Security Center からどのアンチウィルスやセキュリティツールがインストール済なのか認識することが可能になります。

WMI は root¥cimv2 namespace へクエリーを発信することにより、VirtualBox 又は VMware などの仮想環境の存在を見極めることができます。前回サンドボックスの検知回避に関するブログで説明しましたが、マルウェアがセキュリティツール及びサンドボックスの有無を見極めることが可能になると、マルウェアは検知回避するためにずっと沈黙を固持します。

Regsvr32 を利用して検知回避を免れる

他に悪用される正当なツールとしては regsvr32.exe があります。これはデジタル署名の Windows のユーティリティで Dll や Active X 制御などで登録や非登録を行う際に使用される機能です。ファイルの実行時又は regsvr32 経由でモジュールがロードされる場合でも、許可リストツール/既存セキュリティ製品をスルーしてしまうのです。

ある特定の攻撃として Squiblydoo マルウェア（数種類のマルウェアにも組込み採用されて

いる)というのがあり、検知回避テクニックとして他のマルウェアとは異なります。この攻撃はリモートサーバーでホーストされたスクリプトをロード及びランニングする regsrv32 の機能能力を利用します。スクリプトがリモートでホーストされているので、この攻撃は実用的なファイルレス攻撃でステルス性を備えています。

Minerva は自給自足型(LotL)攻撃を先制防御

自給自足型攻撃は正当なネイティブツールを利用して、検知回避をしながら攻撃の脅威を拡散していきます。Minerva はこのような攻撃を防御するモジュールを備えており(特許取得済)、回避手法を阻止することで自給自足型攻撃を無力化しますので、正当なツールを踏み台にして攻撃をされることはありません。

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。