MORPHISEC

MORPHISEC'S 製造業（OT系）のサイバーセキュリティ脅威インデックス

2021年 6月

目　次

はじめに

米国と英国で製造業は約1,500万人を雇用しており、両国の経済に大きな役割を果たしていることは間違いありません。米国のGDP22兆ドルのうち、製造業は約10分の1を占めており、また一方で英国の製造業は世界第9位を誇っています。そのため、以前からサイバー犯罪者が両国の製造業を標的にしていたことは驚くことではありません。その結果として、COVID-19のパンデミックの際には、製造業へのサイバー攻撃が広範囲にわたって増加しました。

パンデミックのピーク時には、企業全体の**攻撃が3倍に増加**し、特に製造業は特に大きな被害を受けました。**製造業は 2020年には、ランサムウェアによる攻撃が最も多かった**と報告されています。製造業は、国家の脆弱性を探り、情報を収集し、金銭を搾取しようとする国家ぐるみのサイバー攻撃に翻弄されることが多くなりました。実際、米英両国の国家安全保障が人々の関心を集めていたこの年、サイバー犯罪者たちは、製造業の主要企業とその重要な知的財産に侵入することで多くの利益を得られると考えていました。

さらに悪いことに、ハッカーは、24時間365日稼働する必要のある製造業を標的にしています。そのため、標的となった企業はシステムのコントロールを取り戻し、ダウンタイムの延長を最小限に抑えるために、すぐにお金を払う可能性があります。ランサムウェアによる被害額は数百万ドルに上り、これらの悪質な関係者がもたらす経済的影響は増加し続けています。

2021年1月にはEmotetボットネットが一掃されましたが、その後、ランサムウェアとインフォスティラ（ホスト内に保存されている機密情報を窃取するマルウェアの種類）を駆使して製造業を狙う、あまり知られていませんがEmotetと同様に攻撃的なサイバー犯罪グループが散見されるようになりました。例えば、コンピュータメーカーのAcerは、今年の3月、REvil/Sodinokibiランサムウェアグループからランサムウェアにより5,000万ドルを要求されました。

製造業が直面しているサイバーセキュリティの脅威の重大性を考慮し、また、製造業の貴重な知的財産を保護するための支援を継続的に行っているMorphisec社は、製造業の攻撃状況に関する社内データと、米国および英国の製造業の従業員567人を対象とした外部調査を行いました。

本レポートは、2021年4月に米国と英国で開催された第1回「Manufacturing Cybersecurity Threat Index」に基づいて作成されました。本レポートでは、この持続的かつ進化し続けるサイバーセキュリティの脅威をより深く掘り下げ、組織の知的財産を標的とした侵害の増加やランサムウェアによる業務停止のリスクが、セキュリティに対する専門家の見解にどのような影響を与えているかを探ることを目的としています。

調査の結果はこちらです。

製造業の脅威の状況

ほとんどの業界と同様に、サイバー犯罪者がパンデミックの影響を受けたオフィスとテレワークと言うハイブリッドな職場環境を標的にすることで、製造業におけるサイバーセキュリティの脅威が、この12ヶ月間で急速に拡大しました。

製造業を標的とした攻撃者は、アローリストに登録されているプロセスを利用することで、ベストプラクティスとしてアローリストに登録された製品や設定を回避することに長けています。このような企業の多くはセキュリティ対策ソリューションを導入していますが、製造業の経営者の中には、自社の知的財産が適切に保護されているかどうか確信が持てない人がまだ多くいます。

Morphisec社は、1月にドイツにある製造業の複数顧客の知的財産を標的とした重大なバンキング・トロイの木馬/インフォスティラ・キャンペーンを発見しました。この例では、標的となった人物は、高度なファイルレスダウンローダーを配信している危険なWebサイトにリダイレクトされ、最終的にC2 onion Torパネルと通信するバンドル型のミニTor付きのOsirisクライアントに誘導されました。

このようなインフォスティラや金銭を目的とした攻撃は、これまでは金融分野でよく見られたものですが、今では製造業の企業がスパイ活動の対象となっています。突発的に攻撃者に短期的な利益をもたらすランサムウェアとは異なり、マルウェアは特定情報へアクセスする長期的な攻撃キャンペーンの一環として展開されます。

エンドポイント

Morphisecが導入されている製造業のエンドポイントに対する攻撃未遂を分析した結果、過去12ヶ月間（2020年3月～2021年3月）では、インフォスティラやバンキングマルウェアの未遂が、それ以前の12ヶ月間に比べて非常に多くなっていました。実際、この期間に試みられた攻撃のうち、インフォスティラとバンキングマルウェアが最も高い割合を占めました（31%）。

次いで、検出中心のアンチウイルスでは阻止できないファイルレス攻撃や未知の攻撃が続きました（28%）。しかし、ファイルレス攻撃の数は過去12ヶ月間と同様であり、この種の攻撃の大きな増加は見られませんでした。一方、エンドポイントに対するランサムウェア（13%）とサプライチェーン（8%）の攻撃未遂は、過去12ヶ月間で顕著に増加しました。

サーバ

Morphisec社の分析によると、製造業の組織内に設置されているサーバに対する攻撃は、前年に比べて、初期アクセスに焦点を当てた悪用が多くなっています。製造業のサーバに対する攻撃の中で最も活発だったのがこのタイプの攻撃（30%）で、BlueKeepやSMBGhostが標的となりました。

製造業のサーバに対する攻撃では、ランサムウェア（15%）も非常に多く利用されていました。これには、ランサムウェアがターゲットのシステムに侵入している間、サイバー犯罪者がランサムウェアを誘導するという、人間が操作するランサムウェアが含まれています。Morphisec社は、これらのケースの中には、サイバー犯罪者がデータを暗号化せずに流出させたケースもあることを確認しており、これは、人間が操作するランサムウェアの攻撃が実際に増加していることを示す新しいパターンを表しています。

米国および英国の製造業従業員を対象とした調査

過去12ヶ月以内にサイバー攻撃を受けたことがありますか？

米国および英国の製造業の5社に1社が、過去12ヶ月間にサイバー攻撃の被害に遭っている。

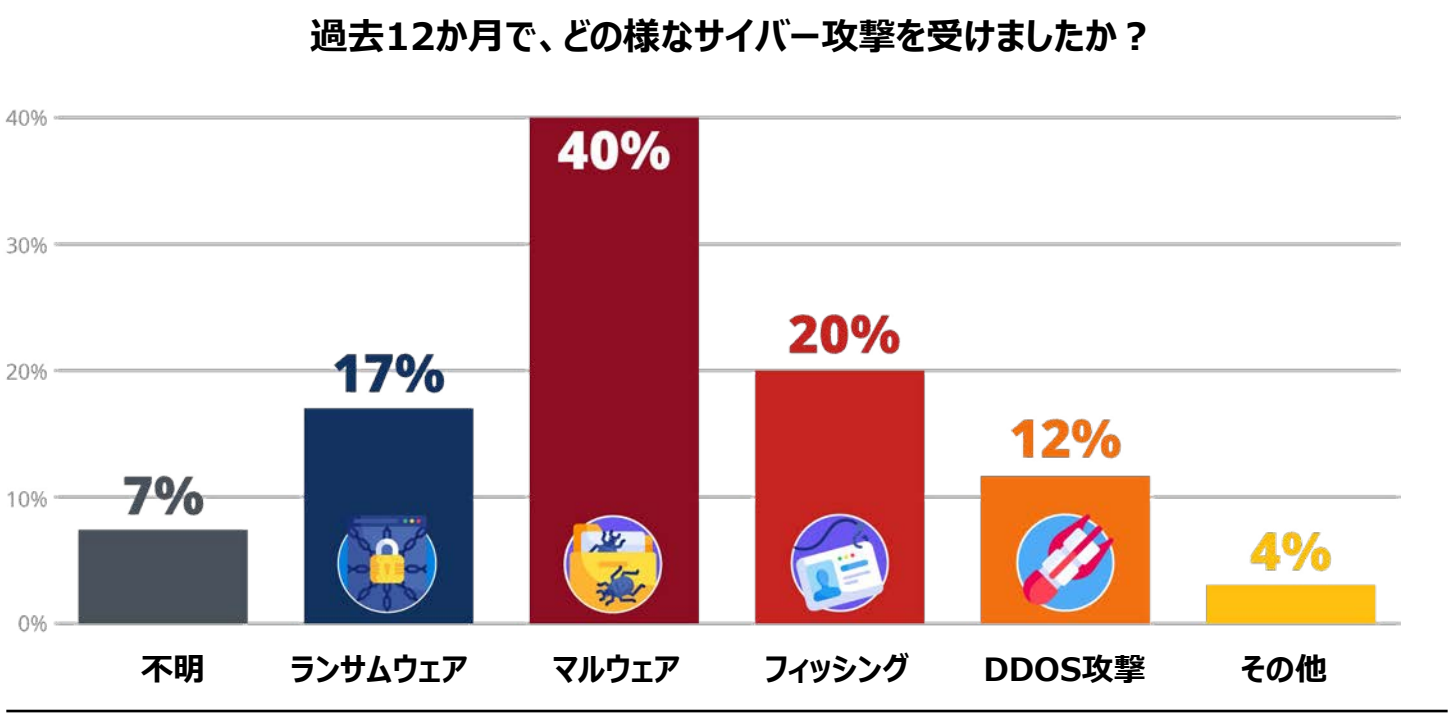
2020年に製造業におけるランサムウェアの攻撃を受けた件数がどの業界よりも多かったと報告していることから、パンデミックの影響への対応に加えて、各組織はサイバーセキュリティ対策を行っていると言ってよいでしょう。この問題は非常に深刻化しており、最近の報告書によると、製造業が支払った身代金の平均額は31万2,000ドルと3倍になり、2020年には過去最高額の1,000万ドルが支払われたとのことです。

当社が米国と英国の製造業従業員567名を対象に行った調査によると、米国と英国にある製造業の5社に1社が過去12ヵ月間にサイバー攻撃の被害に遭っていることが明らかになりました。さらに、これらの攻撃の頻度は増加しています。過去1年間に被害に遭ったと回答した5社中1社のうち、約4分の1（24%）が毎週、35%が毎月サイバー攻撃を受けていると回答しています。

さらに、製造業の専門家全体の70%が、パンデミックの発生以降、製造業がより多くの標的にされていると考えていると指摘していますが、これは当然のことでしょう。結局のところ、製造業は「常に稼働している」業界であり、お金に困っている事業者にとっては魅力的なターゲットであり、利益を上げるためにランサムウェアやマルウェアで情報窃取を行うことを厭いません。このようなサイバー犯罪者は、メーカーにはダウンタイムを発生させる余裕がないという事実を知っています。製造業者はしたがって、被害の拡大を避けるためには、身代金を迅速に支払わなければならないと考えることが多いのです。

しかし実際には、昨年1年間に自社へのサイバー攻撃を報告した製造業関係者の割合は憂慮すべきものですが、それは氷山の一角に過ぎない可能性が高いのです。例えば、Morphisec社の調査によると、調査対象となった製造業の従業員のうち、自社がこれまでにサイバー攻撃を受けたことがあると認識しているのはわずか28%でした。米国と英国の製造業の規模を考えるとかなりの数字ですが、IT部門以外の専門家がすべての攻撃を認識しているわけではないことを考えると、実際の数字はこれよりもはるかに多いと思われます。

米国および英国の製造業従業員を対象とした調査



最も活発な製造業の攻撃の中で、最も被害が大きかったのはインフォスティラとランサムウェアでした。

被害の大きさを考えると、サイバー犯罪者がどのようにして検知を回避し、製造業のネットワークの最も重要な部分にアクセスするのかを理解することが重要です。サイバー犯罪者の動機（利益）はほとんど変わりませんが、攻撃方法は定期的に進化して、ますます巧妙になっています。

先に述べたように、Morphisec社が保有する攻撃状況データによると、過去12ヶ月間に製造業のエンドポイントを狙った攻撃のうち、マルウェアとインフォスティラが約3分の1（31%）を占めており、同社が確認した中で最も一般的な手法でした。また、ランサムウェアよりもインフォスティラの方が2.5倍も利用されていることが分かりました。

製造業の従業員を対象とした調査では、このデータをほぼ裏付ける結果が得られました。過去1年以内に攻撃を受けたと回答した人に、自身の組織が経験した攻撃の種類を尋ねたところ、「マルウェアまたはインフォスティラ」との回答が最も多く（40%）、次いで「フィッシングまたはインフォスティラ」となっています。次いで、「フィッシングまたは詐欺的なビジネスの試み」（20%）、「ランサムウェア」（17%）、「DDoS攻撃」（12%）、「複数の種類の攻撃」（4%）と続きました。

これらの攻撃から製造業の組織が回復するために必要な時間は、ほとんどのケースで最大1週間（53%）、約5分の1（18%）の場合に2週間と回答しています。極端な例では、回答者の5%が攻撃からの復旧に15日から21日を要したと回答し、8%が復旧までの期間はこれよりも長いと回答しました。復旧に3週間以上を要したこれらの最も深刻なケースで注目すべきは、回答者が自分の組織がランサムウェアの被害に遭ったと答えたことです。

米国および英国の製造業従業員を対象とした調査

どんなサイバー攻撃が自組織にとって一番の脅威ですか？

35%

ランサムウェアによる生産の停止、遅延、制限あるいはアクセス不可能

33%

マルウェアあるいはデータ侵害により顧客の情報を漏洩する

20%

マルウェアあるいはデータ漏洩により自社の知的財産が漏洩する

10%

攻撃により生産のIoT機器にアクセスが可能になる

その他 2%

ダウンタイム、顧客情報、知的財産の確保がサイバーセキュリティの最大の関心事

このような深刻な脅威は製造業に限ったことではありませんが、サイバー攻撃者は製造業の施設が保有しているデータを熟知しています。実際、一部のサイバー犯罪グループは、ランサムウェアを知的財産の窃盗を目的としたサイバー攻撃の煙幕として利用し、「金を払わなければデータを流出させる」と脅して被害者をおとしめることで、長期的な被害を拡大させています。

Morphisec社の調査によると、製造業関係者の57%が、自社の組織がサイバー犯罪者に知的財産を狙われることを1年前よりも心配していると回答しており、この懸念は確実に裏付けられています。2月には、カナダのビジネスジェット機メーカーであるボンバルディア社が、ランサムウェアギャング「Clop」のダークウェブポータルで、飛行機や飛行機の部品の設計図が無料で公開されていたことを認めました。

最初の調査では、ボンバルディア社の主要なITネットワークから隔離された専用サーバ上で稼働していたサードパーティ製のファイル転送アプリケーションの脆弱性を利用して、攻撃者がデータにアクセスし窃盗したことが判明しました。また、従業員、顧客、サプライヤーに関する個人情報やその他の機密情報も漏洩しました。

以上のように、知的財産を窃盗されることによる損失についてはよく知られていますが、今回のサイバーセキュリティ危機において、製造業が最も懸念しているのは知的財産ではありません。製造業の専門家が最も心配しているのは、生産活動を停止させ、ネットワークへのアクセスを遅延、制限、または禁止するランサムウェアの攻撃です（35%）。昨年6月、情報漏洩により生産活動にブレーキをかけざるを得なくなったホンダに起こったのは、まさにこれでした。

一方、製造業関係者の3分の1（33%）は、顧客情報を危険にさらすマルウェアやデータ侵害（2015年に下着メーカーのHanesBrands社が受けた90万件の顧客記録を盗む大規模な攻撃のようなもの）が最大の懸念事項であると答えています。次いで、知的財産を侵害するデータ流出（20%）、製造現場のIoT機器にアクセスする攻撃（10%）となっています。

米国および英国の製造業従業員を対象とした調査

パンデミック中、あなたやあなたの製造業の同僚が遠隔地や自宅で仕事をすることで、組織に対するサイバーセキュリティ侵害のリスクが高まったと思いますか？

63% YES  **37% NO**

パンデミックによるハイブリッドな環境での働き方がもたらすサイバー脅威の増大

パンデミックにより何百万人もの従業員が何らかの形で在宅勤務を余儀なくされていることが、このサイバーセキュリティ危機の複雑さに拍車をかけています。それは、製造業においても同様です。製造業の専門家の4分の3以上（76%）が、Morphisec社に対し、「Covid期間中、少なくとも何人かの同僚が遠隔地や自宅で仕事をしたことがある」と回答しています。

しかし、最大手の製造業であっても、ITリソースやセキュリティチームは限られているため、これらの資産がリモート環境に移動すると、セキュリティ設定が複雑になり、既存の脆弱性が悪化してしまいます。例えば、Morphisec社のWFH Employee Cybersecurity Threat Indexによると、リモートワーカーの56%が個人所有のコンピュータを仕事に使用している一方で、4分の1以下は自分のデバイスにどのような対策とネットワークプロトコルがインストールされているかさえ知らないことが明らかになりました。これらの統計は、サイバー犯罪者にとって、弱体化したネットワークをターゲットにして貴重な知的財産に容易にアクセスできる機会を提供するものであり、思わず息を呑むような結果となっています。

その結果、企業のセキュリティ境界線は消失し、攻撃から組織を守るためのITチームの作業は著しく困難になっています。特に、パンデミックが発生して以来、業界全体が、かつてないほどの攻撃の急増に直面していることを考えると、その傾向は顕著です。今回の調査で、遠隔地で働く同僚がいると答えた回答者のうち、約3分の2（64%）が、組織に対するサイバーセキュリティ侵害のリスクが高まったと考えていると答えています。

これらの回答者は、政府機関や民間企業に対する同様の攻撃が後を絶たず、その多くが国家ぐるみで行われているというニュースに影響されていると考えられます。

米国では、わずか数ヶ月間に3回目となる深刻かつ特異なサイバー攻撃が発生し、CISAは最近、緊急指令を出しました。このハッカーは、遠隔地で働く従業員をオフィスに接続するプログラムであるPulse Secureを介してターゲットのデバイスに侵入した後、バックドアプログラムを仕込み、一定期間ネットワークを監視することができました。その結果、米国の主要企業や政府機関にアクセスできるようになりました。

このように米国政府に簡単に侵入できたという事実は、製造業にとっては、セキュリティ対策を強化し、従業員を訓練しなければ被害に遭うリスクがあることを示唆しています。ハイブリッド環境での作業を続ける中で、クラウドサービスへの非効率的な移行や、不適切に保護された企業VPNは、かけがえのない知的財産、従業員や顧客のデータの喪失につながり、もちろん、数百万ドルの損害賠償の可能性もあります。

脅威のプロファイル事例 – 1

Long Live, Osiris: ドイツのIPアドレスを標的としたバンキング・トロイの木馬

脅威

2021年1月、Morphisec社は、ドイツの製造業の複数の顧客を標的とした重要な攻撃キャンペーンを確認しました。この攻撃キャンペーンでは、高度なファイルレスダウンローダーが配信され、最終的にはミニ TorがバンドルされたosirisクライアントがC2 onion Torパネルに通信するようになっていました（現在もそうです）。
追加の調査を行い、TTP（戦術、技術、手順の略）の一部をコミュニティで共有した後、米国や韓国などの追加の標的国について通知を受けました。これらの国では、報告書に記載されているのと同じ配信メカニズムを使用してREvilやその他のペイロードを配信していました。また、その数週間後には、同じTTPによって開始されたCobalt Strikeフレームワークによって危険にさらされた数十社の製造業を確認しました。

訳者注： マルウェアが暗号化した悪意あるコードを解凍し、無害なプロセスを作成し、そのプロセスのコードを悪意あるコードに入れ替える手法

テクニカル分析

攻撃の連鎖は、主に5つのステージで構成されています。

- 被害者は、悪意のあるJSファイルを含んだZIPファイルのダウンロードを行うウェブサイトへのリンクを受け取ります。
  ウェブページとファイル名を翻訳すると、" collective agreement on-call remuneration ig metal." となります。
- 暗号化されたJavascriptダウンローダーを悪意あるサイトから持ち込み、存続し続けるプロセスとしてJavascriptダウンローダーを起動。
- レジストリに書き込まれた前記ファイルレスの.NETローダーでOsirisトロイの木馬を新たに.NETホローに解凍し、正規のWindowsプロセスに組み込みます。（Process Hollowingは左記の訳者注参照）
- Osirisは、ミニ Tor バンドルの助けを借りてそのC2に接続します。
- その後、攻撃者はOsirisをCobaltとREvilに置き換えます。

回避

ドイツのIPアドレスを攻撃するトロイの木馬「Osiris」は、トロイの木馬の本来的な機能を提供しています。Morphisec社のプラットフォームは、エンドポイントセキュリティに関してゼロトラストの考えに基づきデフォルトで拒否する方法でOsirisをブロックします。
Morphisec社の顧客は、攻撃者がどのような防御回避技術を展開しても、Osirisから保護されます。

脅威のプロファイル事例－2

バックドア型 Jupyter Infostealer

脅威

Morphisec社は、2020年11月、日常的なインシデント対応プロセスの中で、Jupyterと呼ばれる新しい.NETインフォスティラの亜種を特定し、防止しました。Jupyterは、主にChromium、Firefox、Chromeのブラウザデータを狙うインフォスティラです。Jupyterは、主にChromium、Firefox、Chromeのブラウザデータを標的としたインフォスティラですが、その攻撃チェーン、配信、ローダーには、完全なバックドア機能のための追加機能があります。これらには以下が含まれます。

- - C2クライアント
- - マルウェアのダウンロードと実行
- - PowerShellスクリプトおよびコマンドの実行
- - 正当なWindows構成アプリケーションにシェルコードを組み込むこと

テクニカル分析

Jupyterの攻撃チェーンは、通常、Docx2Rtfなどの正規のソフトウェアを装った実行ファイルであるインストーラを含むZIPファイルのダウンロードから始まります。このようなインストーラの中には、VirusTotalにおいて過去6ヶ月間に1件も検出されていないものもあり、ほとんどのエンドポイントセキュリティのスキャン制御を回避することができるものもあります。

インストーラを実行すると、.NET C2クライアント(Jupyter Loader)がメモリに注入されます。このクライアントは、明確に定義された通信プロトコル、バージョニング マトリックスを持ち、最近では永続化モジュールも含まれています。

このクライアントは、次の段階として、インメモリのJupyter .NETモジュールを実行するPowerShellコマンドをダウンロードします。どちらの.Netコンポーネントも、コード構造、難読化、独自のUID実装が類似しています。これらの共通点は、インフォスティラを実装するためのエンド・ツー・エンドのフレームワークの発展を示しています。

回避

Morphisecは、2020年5月から複数のバージョンのJupyterを追跡するために、安定したフォレンジックデータを監視してきました。C2の多くはもはや活動していませんが、我々が特定できたときには一貫してロシアにマッピングされていました。

この攻撃がロシア起源である可能性を示す証拠は、これだけではありません。まず、惑星の名前がロシア語から英語に誤記されていることが目立ちます。さらに、Morphisec社の研究員は、C2管理パネルの画像をGoogle画像検索で逆引きしたところ、予想通りロシア語のフォーラムで正確な画像を発見しました。

Jupyterや同様に進化する攻撃は、攻撃者が防御者の先を行くために一貫して攻撃を繰り返すことができることを示しているため、検知を中心としたツールの根本的な問題を明確にしています。Morphisec社のお客様は、ワークステーション、VDI、サーバ、クラウドのワークロード向けのゼロトラストランタイム環境を通じて、攻撃チェーンのどの部分かを検知する必要なく、このような未知の攻撃から保護されています。

脅威のプロファイル事例－3

難読化されたVBScriptから実行するZloader、Ursnif、QakBot、Dridex

脅威

Morphisec社のチームは、2020年3月から、マルウェアキャンペーンの中で難読化されたVBScriptパッケージを追跡するようになりました。当初、このキャンペーンは、ドイツ国内のターゲットに焦点を当てていましたが、ロシアや北朝鮮内のIPアドレスを除いた追加ターゲットへと移行していきました。これらのVBScriptは、以前に確認されたようにZloaderを配信することから始まりましたが、Zloaderに加えてUrsnif、Qakbot、Dridexなどのトロイの木馬を配信するメカニズムへと急速に発展しました。

ここで危険なのは、VBScriptインタープリタがすべてのWindowsオペレーティングシステムにプレインストールされていることで、これはWindows 98以来続いています。VBScript、Javascript、あるいはテキストベースのスクリプトのような解釈される言語は、そのコードが悪意のあるものかどうかをスキャンで判断することが常に困難です。その理由は、同じコマンドや結果を表現するのに、無限の可能性があるからです。

テクニカル分析

Morphisec Labsが追跡したキャンペーンは、ZIP形式の難読化されたVBScriptファイルを電子メールに添付することから始まります。ターゲットが受け取ったメールには、取引金額、日付、取引番号が明記された請求書のようなZIPファイルが添付されています。ここでの目的は、偽の請求書を添付した多くのメールと同様に、ターゲットがメールに注意を払わないようにすることです。

ZIPファイルの添付ファイルの中には、検出率の低い、高度に難読化されたVisual Basic Scriptファイルが入っています。ExecuteGlobalコマンドは、引数として文字列を受け取り、その文字列に含まれるコマンドを実行します。この場合、引数は、数学的な文字操作を用いて文字列に変換される配列の形式になっています。これらの文字列は、後にスクリプトで使用される関数です。この難読化手法は、「ExecuteGlobal」を「Wscipt.Echo」に置き換えることで簡単に抽出できます。

最初の関数呼び出しは、アンチアナリシスとアンチバーチャルマシンに使用されます。以下の回避チェックのいずれかで、仮想マシンや解析環境下で実行されていることが検出されると、攻撃者は知的財産を記録し、スクリプトを削除し、偽のエラーメッセージをポップアップ表示します。また、アーティファクトがあるかどうかをチェックすることで、VBScriptが感染したマシンで実行されているかどうかを確認します。感染したマシン上で実行されていることが検出された場合、偽のエラーメッセージを表示し、スクリプトを削除して終了します。そうでない場合は、感染したマシンに新しいキャンペーンのマークを付けるために、新しいショートカットを作成します。最後に、このスクリプトは、関数のデコードに使用されるのと同じデコード技術を使用して、ペイロードを含むzipフォルダをドロップします。そして、そのフォルダを解凍し、ペイロードを実行します。

回避

VBScriptのようなインタプリタ型言語の単純な難読化、あるいはそれ以下の難読化は、攻撃者がスキャンソリューションを回避するには十分なものです。理由は単純で、これらの言語がテキストベースの言語であるため疑わしいと思われる用語が無限にあるからです。

しかし、どのような難読化を施しても、Morphisecは、Zloader、Ursnif、Qakbot、Dridexなどの回避型ペイロードの実行を、被害が発生する前に防止します。

まとめ

脅威となる人物（＝攻撃者）は、機会を無駄にすることはありません。COVID-19にしても、その他の危機にしても、製造業をターゲットにしたフィッシングメールや標的型フィッシングメールは、組織への侵入の足掛かりを作るためのクリックを促すために、今後も利用され続けるでしょう。企業は、このようなフィッシングメールやその他のタイプのフィッシングメールに注意する必要があります。これらのフィッシングメールは、特定の組織をターゲットにしたものが増え続け、過去の「Spray and Pray」メールのようなものではなくなっていくでしょう。

同様に、ランサムウェアも今後1年間で進化し続けるでしょう。二重搾取攻撃や、ランサムウェアのプログラム自体をキーボードで操作するなど、人間が操作するランサムウェアの傾向が強まることが予想されます。実際、脅威グループが身代金を要求するターゲットに電話をかけて、新しいセキュリティソリューションの導入を思いとどまらせ、確実に身代金を受け取ろうとしているケースもあります。

セキュリティ予算は増加していますが、現実には10年前と比べて安全ではなくなっています。攻撃手法の絶え間ない進化に伴い、悪意のある行為を検知して迅速に修復するのではなく、プロアクティブな防御とゼロトラストのエンドポイント戦略によって攻撃対象領域を減らすことに重点を置いた、新しいアプローチが必要になっています。製造業の企業は、攻撃によって重要なインフラがロックされるリスクを、真に軽減することができなければなりません。

MORPHISECに関して

Morphisecは、特許取得済みのMoving Target Defense（ムービング・ターゲット・ディフェンス）技術により、APT、ゼロデイ、ランサムウェア、回避可能なファイルレス攻撃、Webベースのエクスプロイトなど、企業にとって最も高度な脅威に対して、防御者を防御優先の姿勢にすることで、お客様に全く新しいレベルのイノベーションを提供します。Morphisecは、企業の既存のセキュリティインフラに簡単に導入できる、重要で小さなフットプリントのゼロトラストメモリ防御レイヤーを提供し、今日の攻撃優先の既存サイバーセキュリティモデルを真に破壊する、シンプルで非常に効果的かつコスト効率の高い防御スタックを形成します。