必見!!

最新マルウェアランキング

ランサムウェアについて__進化する現代版ランサムウェアとは？？

ごあいさつ

私たちチェック・ポイント・ソフトウェア・テクノロジーズ株式会社は1993年に創業、世界各国に支店を持つグローバル企業であり、様々なインターネットシーンにおけるセキュリティ対策企業として、官公庁をはじめ数多くの企業様で採用をいただいており、私たちの企業ドメインとして今日に至っております。『サイバー攻撃は大手企業だけ』この様に思われている経営者様も少なくないと思います。『目に見えない脅威だからこそ』私たちはその先にある『財産』『人材』『資産』を守らなければなりません。『100%に近づく安心を』これが私たちの使命であり、企業を守る役割と自負しております。

最新マルウェアランキング

先月ランクダウンしていたけど、以前としてEmotetが脅威を振るってるね!

広報れお

順位	マルウェア	前月比較
1	Qbot	↔
2	Formbook	↑
3	Emotet	↑
4	XMRig	↑
5	AgentTesla	↓
6	GuLoader	↑
7	Nanocore	↑
8	Remcos	↑
9	Tofsee	↑
10	Phorpiex	↑

順位	モバイルマルウェア
1	Anubis
2	Hiddad
3	AhMyth

2月には、リモートアクセス型トロイの木馬（RAT）Remcosが2022年12月以来初めてグローバルのトップ10リストに復活しました。Remcosはウクライナの政府機関を標的にしたフィッシング攻撃に使用されていることが報告されており、1.74%の国内組織にも影響を与えたとして国内ランキングの2位へと順位を上げています。

一方、同じくトロイの木馬型マルウェアのEmotetは3位へと順位を上げました。また、最も攻撃の標的とされている業種・業界は引き続き「教育・研究」分野となっています。CPRによると、ロシアによる侵攻を受けた後のウクライナは、2022年10月から2023年2月にかけて1組織当たりのサイバー攻撃数の週平均は44%減少していることが確認されているものの、現在も依然としてサイバー犯罪者に人気のターゲットとなっていることが報告されています。

直近の攻撃キャンペーンでは、攻撃者がウクライナ国営通信Ukrtelecomになりすまして大量の電子メールを配信し、悪意あるRAR添付ファイルを利用して、2022年12月以来初めてトップマルウェアのリストに復帰したトロイの木馬、Remcosを拡散しています。Remcosのツールがインストールされると、侵害されたシステム上にバックドアが作成されてリモートユーザーのフルアクセスが可能になり、データ流出やコマンドの実行などの活動ができるようになります。現在報告されている攻撃は、インシデントの行動パターンや攻撃能力から、サイバー領域におけるスパイ活動との関連があると考えられています。

チェック・ポイントのリサーチ担当であるマヤ・ホロウィッツ（Maya Horowitz）は、「政治的な動機によるウクライナへの攻撃は減少していますが、それでもウクライナがサイバー犯罪者の戦場と化していることに変わりはありません。ロシアとウクライナの戦争が始まって以来、脅威アクターたちはハクティビズムを優先的に実行しています。多くの場合、DDoS攻撃のようなより妨害的で混乱を招く攻撃方法を好んで使用しており、高い注目を集めることにも成功しています。しかしながら、最新の攻撃キャンペーンではより従来に近い攻撃ルートが使用されており、フィッシング詐欺を利用してユーザー情報を取得し、データを抜き取るという手が使われています。あらゆる組織や政府機関にとって、電子メールを受信したり開いたりする際には、安全なセキュリティ対策の手順を順守することが重要です。決して、内容をスキャンする前に添付ファイルをダウンロードしないでください。メール本文内のリンクはクリックを避け、送信者アドレスに余計な文字やスペルミスなどの異常がないかを確認しましょう」

日本国内のマルウェアランキングも見て、しっかりと対策を考えよう!!

広報れお

国内マルウェアランキング

*矢印は、前月と比較した順位の変動、（）内の数字は国内企業への影響値を示しています。

国内ランキングでは、1月に3.80%の国内企業に影響を与え3位だったQbotが2月には1位へ順位を上げています。また 昨年国内でも猛威を振るったEmotetが12月以来の2位となっています。

1.　↑**Qbot (4.07%)** - Qbot、別名Qakbotは、2008年に初めて発見されたバンキング型トロイの木馬で、銀行の認証情報とキーストロークを盗み出すよう設計されています。スパムメールを通じて拡散されることが多く、アンチVM（仮想マシン）、アンチデバッグ、アンチサンドボックスなど複数の手法を用いて解析を妨げ、検知を回避します。

2.　↑**Emotet (1.74%)** – Emotetは自己増殖する非常に高度なモジュール型トロイの木馬です。かつてはバンキング型トロイの木馬として使用されていましたが、最近では他のマルウェアの拡散や悪質なキャンペーンにも使われています。Emotetは持続性を維持する様々な手段と、検知を免れるための回避技術を搭載しており、悪意ある添付ファイルやリンクを含むフィッシングメールを介して拡散されます。

同2.　↑**Remcos (1.74%)** – 2016年に初めて出現したRATです。Remcosは、SPAMメールに添付される悪意のあるMicrosoft Office文書を通じて配布されます。Microsoft WindowsのUACセキュリティを回避し、高レベルの特権でマルウェアを実行するよう設計されています。

同2.　↑**XMRig (1.74%)** – XMRigは、仮想通貨Moneroのマイニングに使用されるオープンソースのCPUマイニングソフトウェアです。脅威アクターは多くの場合、このオープンソースソフトウェアをマルウェアに組み込み、被害者のデバイス上で違法なマイニングを行う形で悪用します。

ランサムウェアについて考える

先月号のCheck_NEWSでも少しだけ話をしていたランサムウェア。現在世界中で脅威を振るっており、日本国内においても、2022年10月末に大阪急性期・総合医療センターが被害に遭い、大きな話題となりました。今回はこのランサムウェアについて深掘りしていきたいと思います。

狙われる医療・教育機関

先述したマルウェアランキングでも掲載していますが、教育、医療関係はマルウェアの被害に遭いやすい業種です。なぜ、そのような機関が狙われやすいのか？
それは、**センシティブ**な情報を持っているからだと考えられます。一旦ランサムウェアに感染し、暗号化されてしまうと、病院の場合電子カルテの閲覧が出来なくなり、診療自体がストップ、病院としての機能が停止してしまいます。身代金を支払ったとしても復旧する見込みはありませんが、被害を受けた身から考えると、支払って解決するのであれば・・。という心理に陥ってしまうのでしょう。

進化するランサムウェア

世界最初のランサムウェアと言われる「ＡＩＤＳ Trojan」が1989年12月に見つかってから約35年、2008年にはWinLocker、2011年の「Reveton」、そして現在のランサムウェアにおける原型とも言える2013年に猛威を振るった、「CyptoLocker」、世界中を震撼させた、2017年の「WannaCry」と、ランサムウェアは日々進化していることも忘れてはなりません。

今までのランサムウェア

WannaCryなど

対象	主にクライントのパソコンや サーバー
症状	ファイルの暗号化・身代金の要求
被害額	数万円

最近の新型ランサムウェア

REvil/Ryukなど

対象	パソコン・サーバー・制御系のシステムなど
事象	Active Directoryを乗っ取り、企業ネットワークの制御を管理下に置く、その後にファイルサーバ、やPCの暗号化及び情報窃取
目的	暗号化解除のために身代金要求、さらに窃取情報の公開を止めるための身代金要求 窃取した情報を他社に販売するケースも
被害額	数千万円～

3.　↑SnakeKeylogger (1.45%) – 2020年11月末に初めて発見されたSnakeKeyloggerは、モジュール型の.NETキーロガー、そして認証情報の窃取ツールであり、主な機能は、ユーザーのキーストロークを記録し、集積したデータを脅威アクターに送信するというものです。このマルウェアは特に回避性能が高く、あらゆる種類の機密情報を盗むことが可能であるため、ユーザーのオンラインにおける安全性に対し、大きな脅威となります。

グローバルで活発な上位のマルウェアファミリー

*矢印は、前月と比較した順位の変動を示しています。
2月、世界的に最も流行したマルウェアはQbotで、全世界の組織に7%以上の影響を与えています。2位はFormbookで世界的な影響は5%、3位はEmotetで影響は4%でした。

1.　↔ Qbot – 国内ランキングと同じく、世界的にも2023年2月に最も活発だったマルウェアとなりました。2022年12月からグローバルランキングにおいては、3ヶ月連続で1位にランクインしています。

2.　↑ FormBook – FormBookはWindows OSを標的とするインフォスティーラーです。2016年に初めて検知されたこのマルウェアは、強力な回避技術と比較的安価な価格から、ハッキングフォーラムでは「Malware-as-a-Service（MaaS）」として販売されています。FormBookは様々なWebブラウザから認証情報を集積し、スクリーンショットを収集し、キーストロークを監視・記録します。また、C&C（コマンド＆コントロール）サーバの命令に従ってファイルをダウンロードして実行します。

3.　↑ Emotet – Emotetは自己増殖する非常に高度なモジュール型トロイの木馬です。かつてはバンキング型トロイの木馬として使用されていましたが、最近では他のマルウェアの拡散や悪質なキャンペーンにも使われています。Emotetは持続性を維持する様々な手段と、検知を免れるための回避技術を搭載しており、悪意ある添付ファイルやリンクを含むフィッシングメールを介して拡散されます。

世界的に最も攻撃されている業種、業界

2月、世界的に最も攻撃されている業界は「教育・研究」でした。2位は「政府・軍関係」、3位は「保健医療」となっています。

1. 教育・研究
2. 政府・軍関係
3. 保健医療

モバイルマルウェアのトップ

2月も引き続きAnubisが最も流行したモバイルマルウェアとなり、2位にHiddad、3位にはAhMythが続いています。

1.　Anubis – AnubisはAndroidデバイスを標的として設計されたバンキング型トロイの木馬です。最初に検出されて以来、リモートアクセス型トロイの木馬（RAT）としての機能、キーロガーや音声録音、ランサムウェアが持つ様々な機能など、多くの機能が追加されています。AnubisはGoogleストア上で公開されている数百種類のアプリから検出されています。

2.　Hiddad – HiddadはAndroid端末向けのマルウェアで、正規のアプリケーションをリパッケージし、サードパーティーのアプリストア上で公開しています。主な機能は広告の表示ですが、OSに組み込まれた重要なセキュリティデータにアクセスすることも可能です。

3.　AhMyth – AhMythは、2017年に発見されたリモートアクセス型トロイの木馬（RAT）です。アプリストアや各種ウェブサイト上で公開されているAndroidアプリによって配布されています。ユーザーがこのマルウェアに感染したアプリをインストールすると、マルウェアはデバイス上で機密情報を収集し、キーログやスクリーンショットの撮影、SMSメッセージの送信、カメラの起動など、機密情報を盗み出すためのアクションを行います。

Check_NEWS Vol. 3
令和５年３月

必見!!

最新マルウェアランキング
ランサムウェアについて__進化する現代版ランサムウェアとは？？

安全と言われていたVPNが狙われる

ランサムウェアに感染する経路として、主に2種類があげられます。一つは不審なメールの添付ファイルを開封することで発症してしまう事例。そして、もうひとつの事例がVPNを利用したランサムウェア感染事例です。

メールを使った手口についても、2021年1月にEUROPOL（欧州刑事警察機構）がEmotetのテイクダウンに成功し、Emotetは一時期活動を停止していたものの、2021年11月に活動を再開したことが報じられています。

さて、今回はVPN経路についてを図解にて説明したいと思います。おそらく10年以上前、VPNは安全だ！と言われていたと思います。

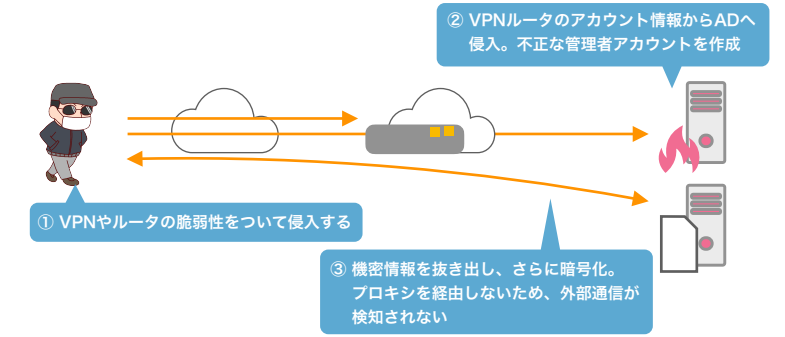
しかし、そのVPNの脆弱性や機能を利用したランサムウェアの被害が日々増えています。

今回はその事例をもとに図解で説明をしたいと思います。

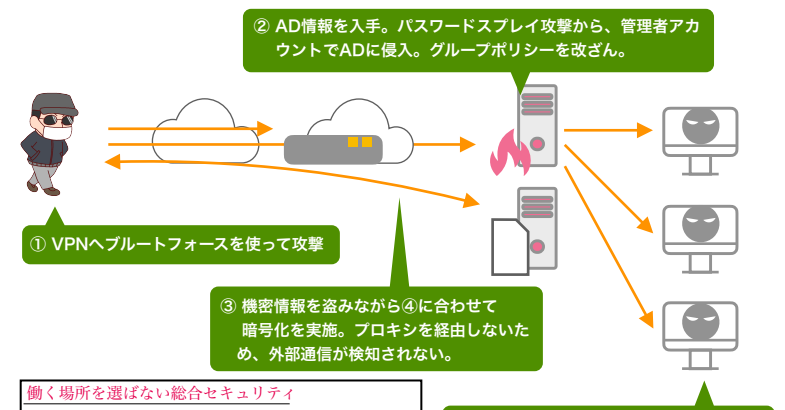
『我々は安全だ』
『我々みたいな会社は狙われることはない』
と、お思いの方も少なくないと思います。

是非下記事例を参考にしながら、対策を練ってください。

VPN被害事例 1　脆弱性をついて侵入する



VPN被害事例 2　ブルートフォースを使ったアカウント搾取



チェック・ポイント・ソフトウェア・テクノロジーズ株式会社　URL：https://cp-smb.com
〒105-0001東京都港区虎ノ門1-2-8虎ノ門琴平タワー25F