2020年10月27日

NEWS RELEASE

キヤノンマーケティングジャパン株式会社

「Avaddon」ランサムウェアの解析レポートを公開
数多くの攻撃バリエーションを持ち進化する実態を確認

キヤノンマーケティングジャパン株式会社（代表取締役社長：坂田正弘、以下キヤノンMJ）は、最近流行している情報公開型のランサムウェア「Avaddon（アヴァドン）」の解析レポートを公開しました。今回の解析結果では、Avaddonを用いた日本国内を標的とする攻撃が確認されました。さらに、これまで明らかになっていないバージョン間の差異を発見し、Avaddonが数多くの攻撃バリエーションを持ち、進化を続けているその実態も確認しました。

Avaddonは RaaS（Ransomware as a Service）として提供されている情報公開型（暴露型）ランサムウェアです。数多くの攻撃バリエーションが存在しており、複数の攻撃者がサービスを悪用していると考えられます。ランサムウェアはパソコンなどの端末やサーバー上のデータを暗号化し使用不可にすることで、企業の事業継続に対する脅威となっています。加えて、Avaddonを含む情報公開型と呼ばれるランサムウェアのサービス提供者は、暗号化前に窃取した機密情報をWebサイトで公開するという二重の脅迫（double extortion）と呼ばれる手法で、被害者からさらなる金銭を要求します。

キヤノンMJは、2020年6月9日以降にAvaddonの拡散を狙ったメールが日本のアドレス宛に多数送信され、日本国内を明確に標的とした攻撃が仕掛けられたことを確認しました。

さらに、キヤノンMJによる独自の情報収集、分析により、これまでに明らかになっていないAvaddonにおけるバージョン間の差異を発見しました。ファイルを暗号化するだけではなく、さまざまな機能を持ち、複数の攻撃バリエーションの存在を確認しています。この度公開したレポートでは、Avaddonが持つ機能を解析した結果や、新たに発見したバージョン間の差異を詳細に解説しています。

○「Avaddon」ランサムウェアの解析レポート
【https://eset-info.canon-its.jp/malware_info/trend/detail/201027.html】

マルウェアなどのインターネット上の脅威は日々高度化・巧妙化が進み、法人、個人を問わず金銭的被害や機密情報の漏えいなどリスクが増大しています。このような状況においては、被害に遭わないために最新動向を知り、適切なセキュリティ対策を実施することが重要です。

キヤノンMJグループはセキュリティソリューションベンダーとして、サイバーセキュリティに関する研究を担うサイバーセキュリティラボを中核に、最新の脅威やマルウェアの動向の情報収集および分析を実施しています。さらに、セキュリティ対策に必要な情報をレポートとして発行し、国内のセキュリティ対策の立案を支援しています。

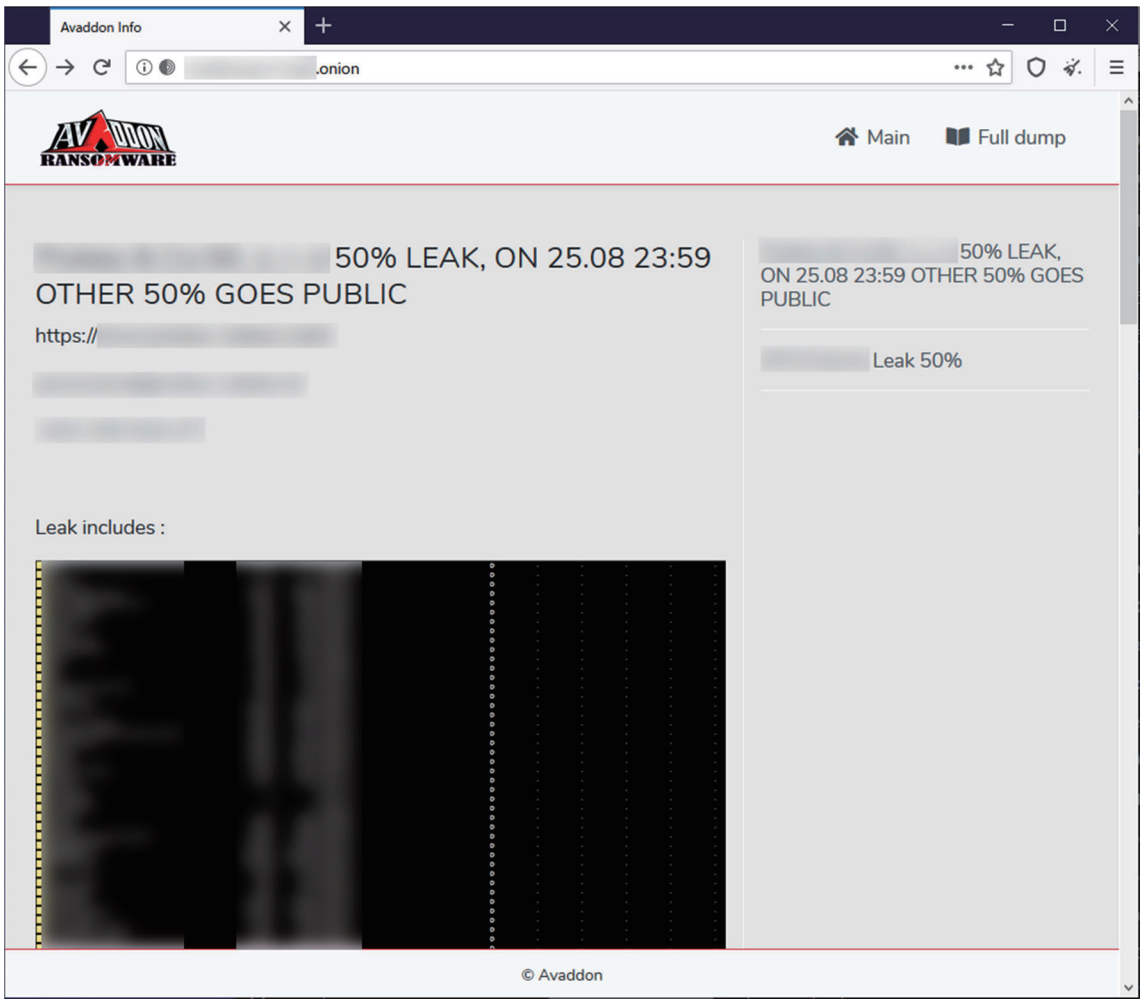
● 報道関係者のお問い合わせ先：キヤノンマーケティングジャパン株式会社
広報部 パブリックリレーションズグループ　03－6719－9093（直通）
● 一般の方のお問い合わせ先　：セキュリティソリューション事業企画第二課　03－6701－3452
● マルウェア情報局ホームページ：https://eset-info.canon-its.jp/malware_info/
● ニュースリリースホームページ：canon.jp/newsrelease

＜“Avaddon ランサムウェアの解析レポート”の主な内容＞

■ 情報公開型（暴露型）のランサムウェア「Avaddon」

Avaddon は RaaS（Ransomware as a Service）として提供されているランサムウェアです。Avaddon ランサムウェアを使った攻撃は数多くのバリエーションが確認されており、複数の攻撃者がサービスを利用していると考えられます。

2020年8月に、Avaddon のサービス提供者は窃取した機密情報を公開するための Web サイトを立ち上げています。これは二重の脅迫（double extortion）と呼ばれる手法で、被害者からさらなる金銭を要求するために Avaddon だけでなく、Maze や Nemty 等多くのランサムウェアで採用されています。

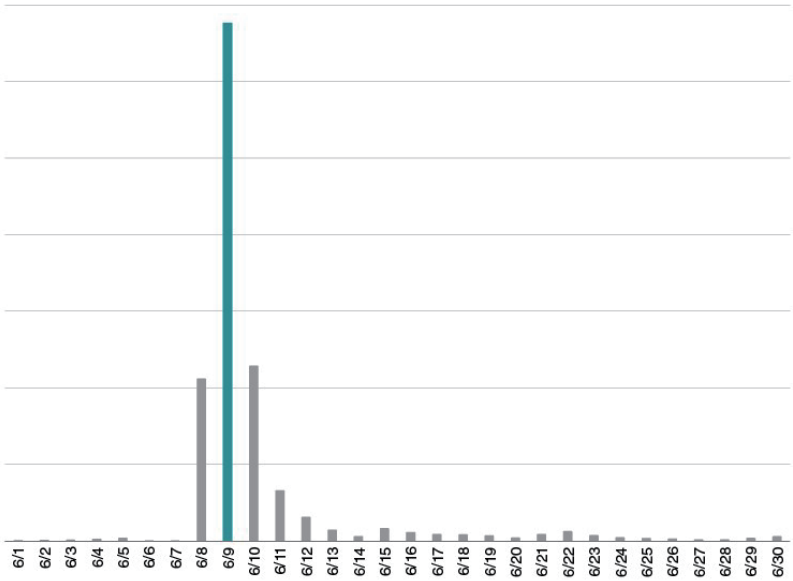


Avaddon の情報公開脅迫 Web サイト

■ 日本国内に向けた攻撃を確認

Avaddon ランサムウェアの感染経路は複数確認されていますが、多くの拡散に使われたのが2019年の初め頃に登場したボットネット「Phorpiex」です。

2020年6月5日頃、Phorpiex ボットネットを使用した Avaddon ランサムウェアの拡散は始まり、6月9日には日本のメールアドレス宛にメールが多数送信され、日本をターゲットにした攻撃を仕掛けたと考えられます。このメールは ESET 製品で JS/Danger.ScriptAttachment として検出されています。

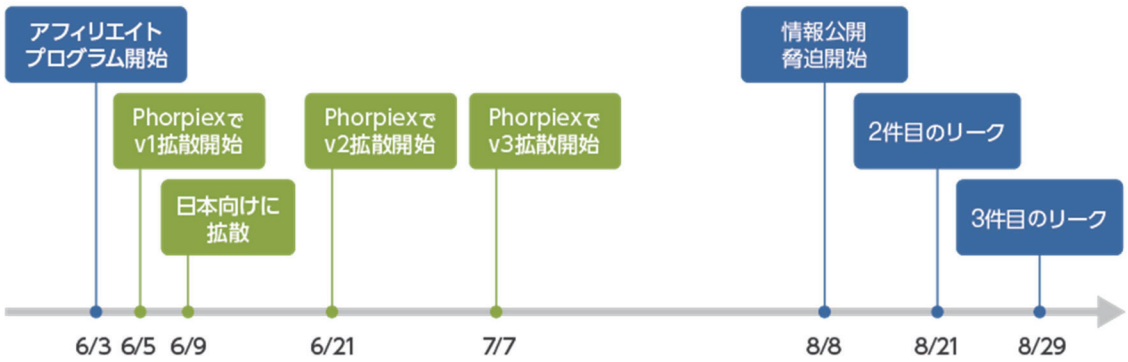


JS/Danger.ScriptAttachment の日別検出数の推移（2020年・日本国内）

■ バージョン間における差異を発見

Avaddon はいくつかの文字列を暗号化してプログラム内部に保持しており、その暗号化（復号）方法は複数のバリエーションが確認されています。

また、Avaddon ランサムウェアはファイルを暗号化するだけではなく、動作している環境の検知、ファイル復元の防止、ランサムノートの作成など、複数の機能を持っており、バージョン間で差異があることを発見しました。本レポートでは Avaddon が持つさまざまな機能について解析の結果を詳細に解説しています。



Avaddon に関連するイベントのタイムライン

■ マルウェアやセキュリティに関する情報を「マルウェア情報局」で公開中

キヤノン MJ では、インターネットをより安全に活用するために、マルウェアや各種セキュリティに関する情報を提供しています。こちらも合わせてご覧ください。

マルウェア情報局
【https://eset-info.canon-its.jp/malware_info/】

マルウェア情報局は、キヤノン MJ が日本国内総販売代理店として取り扱う ESET 製品に関する情報や、マルウェアの情報を提供するポータルサイトです。本サイトでは、スロバキアのセキュリティベンダー ESET 社が発信するニュースを中心に、キヤノン MJ のサイバーセキュリティに関する研究を担うサイバーセキュリティラボが発信するレポートを掲載しています。