2020年11月20日

NEWS RELEASE

キヤノンマーケティングジャパン株式会社

フィッシングメールによって拡散された「Dridex」ダウンローダーの解析レポートを公開

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、2020年に多数検出が確認されたダウンローダー「Dridex（ドライデックス）」の解析レポートを公開しました。今回の解析結果では、さまざまな形式のダウンローダーや数多くの解析妨害の仕組みによって、巧妙に端末へ侵入し検出を困難にさせる実態を確認しました。

キヤノンMJは、2020年日本国内においてDridexの感染を狙ったダウンローダーを複数確認しました。Dridexはボットネットを形成するバンキングマルウェアです。主な侵入経路はフィッシングメールであり、感染するとオンラインバンキングなどの認証情報や機密情報が窃取されます。

今回の解析結果により、従来のDridexダウンローダーに比べ、Excelファイル、Wordファイル、VBSファイルなど様々な形式が存在することが判明しました。さらにDridexダウンローダーは、あまり利用されていないVBAのレイアウトを利用したり、環境により動作が異なったりするなどさまざまな仕組みが施されており、セキュリティソフトの検知を避け、解析を妨害する狙いがあることが明らかになりました。

本レポートでは、Dridexの主な侵入経路となるフィッシングメールと添付されたダウンローダーの動作について、2020年4月と7月にそれぞれ確認された特徴や違いなどを紹介します。

○フィッシングメールによって拡散されたDridexダウンローダーの解析レポート

【https://eset-info.canon-its.jp/malware_info/trend/detail/201120.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

＜“フィッシングメールによって拡散されたDridexダウンローダーの解析レポート”の主な内容＞

■2020年に日本国内でDridexの感染を狙ったダウンローダーを多数確認

2020年、Dridexの感染を狙ったダウンローダーを数多く確認しています。
4月に日本で検出したVBA/TrojanDownloader.Agent（VBAを悪用したダウンローダー）を確認したところ、上位の亜種のほとんどがDridexの感染を狙ったダウンローダーでした。確認した亜種だけでもVBA/TrojanDownloader.Agent全体の80%近くを占めていました。また7月においてもDridexの感染を狙ったダウンローダーが引き続き確認されています。

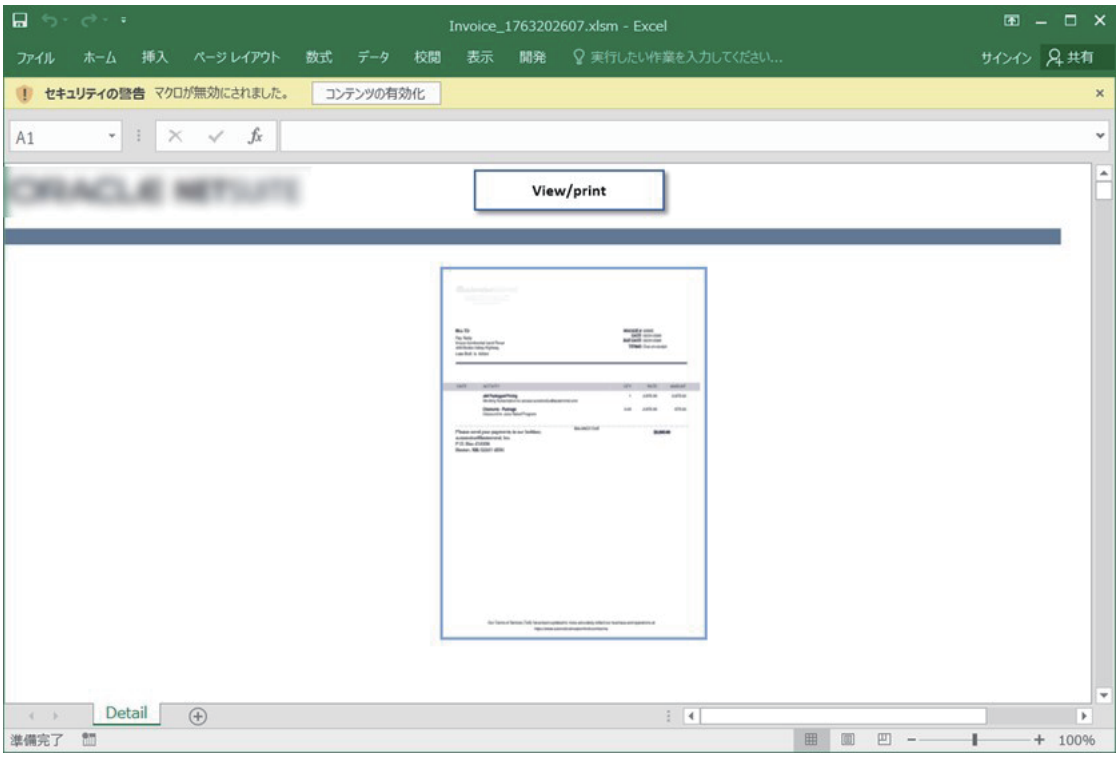
■ 複数の形式のダウンローダー

Dridexのダウンローダーには、Excelファイル形式、Wordファイル形式、VBSファイル形式など様々な形式が存在します。

2020年4月、7月には、実在する複数の運送会社を装ったフィッシングメールや請求書を装ったフィッシングメールを確認しています。4月に確認された実在する運送会社を装ったメールでは、添付されているファイルを開くと、請求書を装った画像が表示され、そこからコンテンツの有効化をクリックするとWMI経由で実行されたPowerShellよりダウンロードされたDridexに感染します。

7月には、請求書を装ったダウンローダーが添付されたフィッシングメールが確認されました。そのメールに添付されているファイルを開き、コンテンツを有効化すると、Excelのプロセスから直接Dridexをダウンロードし、実行します。

本レポートでは、それぞれのダウンローダーの動きやDridex感染までの流れを詳細に解説しています。



正規の企業からの請求書を装ったダウンローダー（※一部モザイク処理を施しています）

■ さまざまな解析妨害の仕組み

Dridex ダウンローダーで利用されている VBA ソースコードには、あまり利用されない Layout イベントを利用して自動実行を行い、セル内から抽出した文字列をデコードして実行する処理が記載されているものもありました。これは、セキュリティソフトの検知を避ける狙いや解析を妨害する狙いがあるものと考えられます。

ダウンローダーが接続を試みる URL は、エンコードされた大量の URL リストから選択されます。これは自動解析や動的解析により抽出された URL がシグネチャに登録される確率を減らしている可能性があります。一部の URL への通信がブロックされていても、ブロックされていない URL が存在すればダウンロードが成功し Dridex に感染する可能性があります。

本レポートでは Dridex ダウンローダーのさまざまな解析妨害の仕組みについて詳細に解説しています。

```
>>> for url in urllist.replace("¥t","").split("¥n"):
...   print("".join([chr(ord(c) + ord("h") - ord(url[0])) for c in url]))
...
https://he           mlas.se/ukef26.txt
https://he           mlas.se/y0bvsc.pdf
https://bol          ilmdirector.com/ib9tfm.txt
https://le           ewouavie.com/p8yljj.txt
https://za           e.pl/ge9arn.txt
https://le           ewouavie.com/x4mkyo.pdf
https://za           e.pl/v7f6l4.pdf
https://he           mlas.se/fojik1.rar
https://bol          ilmdirector.com/e6xbxo.pdf
https://gd           /j7sumb.txt
https://le           ewouavie.com/legxmb.rar
https://bol          ilmdirector.com/nqd7dd.rar
https://za           e.pl/knpyhq.rar
https://po           e.in/3zqpkh.txt
https://li           ser.com/1zg5cb.txt
https://pl           ing.co.uk/5v3k2o.txt
https://he           mlas.se/g8mtcq.rar
https://na           /xtfi4j.txt
https://lo           /rkhmzt.txt
https://ma           tha.net/wpn57i.txt
```

URL リストのデコード処理

■ 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。