2022 年 1 月 17 日
デジタルアーツ株式会社

PRESS RELEASE

マルウェアに悪用されるファイル共有サービスに要注意
～「Discord」や「OneDrive」の正規 URL でも油断できない～

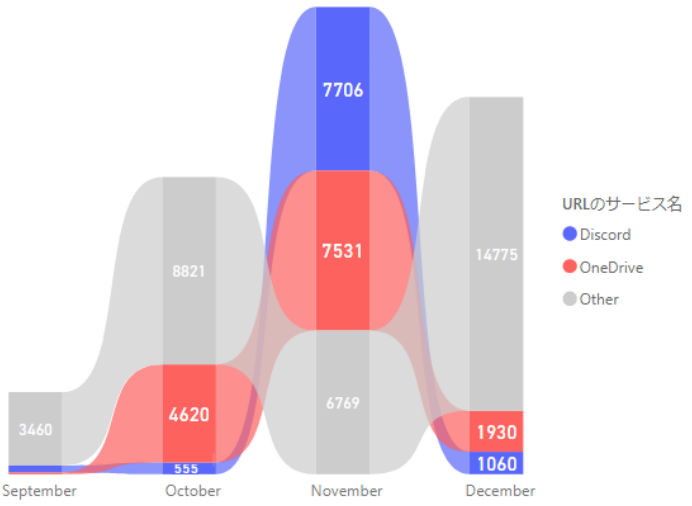
情報セキュリティメーカーのデジタルアーツ株式会社（本社：東京都千代田区、代表取締役社長：道具　登志夫、以下 デジタルアーツ、証券コード 2326）は、マルウェアに悪用されるファイル共有サービスについてのセキュリティレポートを公開したことを発表いたします。

マルウェアに悪用されるファイル共有サービス「Discord」、「OneDrive」

ファイル共有サービスは大容量データの共有や PPAP（パスワード付き ZIP でのファイル運用）の代替策などとして多くの企業で利用されていますが、こうしたファイル共有サービスがマルウェアに悪用されていることはご存知でしょうか。具体的な手口としては、正規のファイル共有サービスにマルウェアを仕込んだファイルをアップロードし、その悪用 URL をメールやメールの添付ファイルで拡散することで、マルウェア感染を広げるというものです。こうしたファイル共有サービスの悪用は以前から行われていました。

マルウェアの配布に使用された悪意ある URL を共有するプロジェクト「URLhaus」における 2021 年 9 月から同年 12 月末までの 4 カ月間で報告された URL をもとに、デジタルアーツが URL のサービス名を分類したところ（IP アドレス形式は除外）、2021 年の年末にかけては「Discord」と「OneDrive」の 2 サービスの URL が突出して悪用されていたことがわかりました。

悪用URL数とサービス



	September	October	November	December
Discord	330	555	7706	1060
OneDrive	80	4620	7531	1930
Other	3460	8821	6769	14775

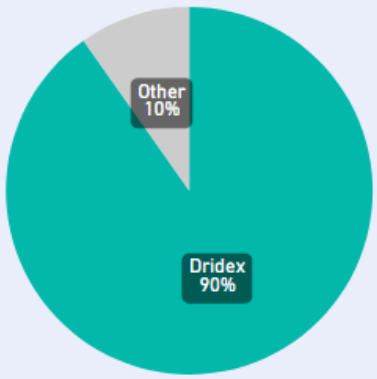
（※）2021年9月～12月 URLhausより。IPアドレス形式のURLは除く。

実質的なファイル共有サービスとして悪用される Discord

Discord は無料で利用可能なコミュニケーションアプリです。PC やモバイルの各種 OS に対応し、専用アプリだけでなく Web ブラウザからも通話・ビデオ・テキストチャットの利用が可能で、世界で広く利用されています。チャットメッセージでファイルを共有することも可能で、その共有したファイルにはそれぞれ URL が生成され、URL を知っていれば誰でもそのファイルを閲覧・ダウンロードすることができます。しかし、実質的にファイル共有サービスのように URL を用いた共有が可能なため攻撃者にも悪用されています。URL は下のような形式です。

hxxps://cdn.discordapp[.]com/attachments/チャンネル ID/ファイル ID/ファイル名

Discordを悪用していたマルウェア



（※）2021年9月～12月 URLhausより

Discord のファイル共有 URL を用いて感染を拡げようとしていたマルウェアは Dridex が非常に多く、報告された Discord の URL の 9 割以上を占めています。

以前に本セキュリティレポートで取り上げた Dridex※1 では改ざんサイトの URL を大量に悪用していました。今度は改ざんサイトではなく、正規の Discord のファイル共有 URL を用いるものが目立つようになっています。

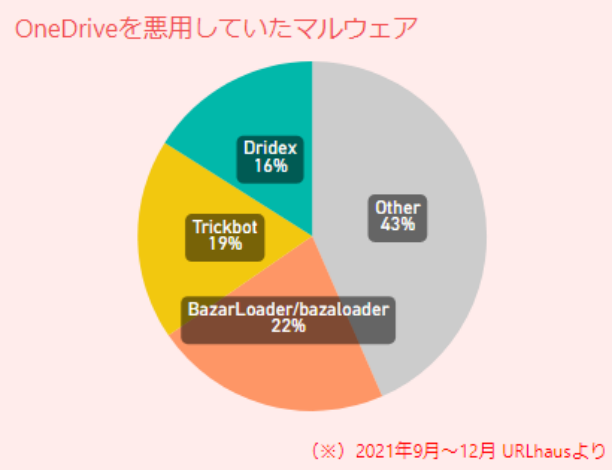
さらに、Excel-DNA で作成された XLL ファイル※2 を使っていたことも確認しました。一度に 150 もの Discord の URL が使われることもあります。人気ドラマに乗じたスパムメールでの拡散も確認しています。ドラマの続編を先取りして観られるなどといってメールで誘い、添付のファイルを開かせようとします。ファイルを開いた後にマクロを有効にして実行してしまうと、Discord に置かれたマルウェアをダウンロードして Dridex 感染へと至るような仕組みです。

OneDrive の悪用

OneDrive は、Microsoft のクラウドストレージです。Windows 10 や Windows 11 ではデフォルトでアプリがインストールされているため一般的に利用されている方も多いのではないでしょうか。

これまで、OneDrive が悪用されるのは珍しいことでもなかったのですが、10 月に入り一気に増加しました。OneDrive の URL には、
api.onedrive.com/onedrive.live.com/files.1drv.com/1drv.ms
というドメインが用いられており、各ドメインは正規のものです。

2021 年 10 月に海外のリサーチャーたちが、OneDrive（Microsoft）側がなかなか対処しないために悪性ファイルの URL が何日も生存し続けていると問題視していました。さらに海外 IT 系メディアもこれを取り上げ、一時話題となりました。その後、OneDrive 側での対処が迅速になっています。



ビジネスで使わないサービスはフィルタリングでアクセスさせない、メールのセキュリティ対策も重要

Discord は Dridex での悪用が目立っていますが、それ以外にも多くの攻撃者・マルウェアによって悪用されています。OneDrive も同様です。サービス提供側も悪用への対処はしているでしょうが、ファイルや URL が迅速に対処され無効になったとしても攻撃者側は使い捨てにして新たに作成すればよく、いたちごっこになっていることは否めません。

近年、国内では PPAP 廃止の動きが加速し、ファイル共有サービスを取り入れた運用に切り替えている組織が増えているようです。正規サービスの URL だからといって単純には安心はできません。今回、突出して悪用された Discord や OneDrive は個人利用の多いサービスです。ビジネスで使わない不要なサービスは URL フィルタリングを活用してアクセスさせないことが大切です。また、メールゲートウェイで添付ファイルや送信元アドレスなどから安全ではないメールはあらかじめ弾くといったセキュリティ対策を講じることも重要です。

▼デジタルアーツは、フィルタリングによるオンラインストレージの利用制御、ホワイト運用、脱 ZIP 暗号化を提案

■「i-FILTER」Ver.10 では、ファイル共有サービスのブロックが可能です。Discord（cdn.discordapp.com）は[チャット][インターネット電話]、OneDrive（api.onedrive.com/onedrive.live.com/files.1drv.com/1drv.ms）は[オンラインストレージ]としてカテゴリ分類しており、カテゴリによるフィルタリングが可能です。さらに OneDrive は「Web サービス制御機能」によって対象サービスだけの細かな制御が可能です。

■「i-FILTER」Ver.10 ・「m-FILTER」Ver.5　セキュリティ対策の新定番 ホワイト運用
受信したすべてのメールを開け、アクセスしたい Web をクリックでき、情報システム部門の運用負荷も削減できます。デジタルアーツの「ホワイト運用」がセキュアな世界を実現します。

■PPAP は効果がないのか？Emotet や IcedID などの外部攻撃対策にはデジタルアーツの『脱 ZIP 暗号化』運用
メールでファイルを送る際に、日本の多くの企業・団体で慣例化された PPAP ですが、セキュリティレベルを担保するための暗号化ではないため、さまざまなインシデントリスクを抱えてきました。デジタルアーツでは、これら「ZIP 暗号化」運用のリスクに対していち早く警鐘を鳴らし、解決しています。

▶マルウェアに悪用されるファイル共有サービスについてのレポートはこちら

以下、弊社コーポレートサイト上にて公開しております。
セキュリティレポート https://www.daj.jp/security_reports/220117_1/

※1 セキュリティレポート「メール経由で感染を狙う Dridex キャンペーン 大量の改ざんサイト URL を悪用」
https://www.daj.jp/security_reports/210309_1/

※2 セキュリティレポート「見慣れない XLL ファイル（Excel アドイン）を使う攻撃が増加中」
https://www.daj.jp/security_reports/211005_1/

デジタルアーツ株式会社 概要

Web、メール、ファイルなどのセキュリティソフトウェアの提供を核に事業展開する情報セキュリティメーカーです。
1995 年の創業以来、「より便利な、より快適な、より安全なインターネットライフに貢献していく」を企業理念とし、有害情報の閲覧を制限する Web フィルタリングソフトを開発、以来企業・公共・家庭向けに情報セキュリティ製品を提供しております。

東京都千代田区大手町 1-5-1 大手町ファーストスクエア ウエストタワー14F ▶URL: https://www.daj.jp/
＜本リリースに関するお問い合わせ＞
デジタルアーツ株式会社 広報担当 山田 TEL : 090-1555-7254 / E-mail : press@daj.co.jp
※新型コロナウイルス感染症拡大に伴う在宅勤務実施中のため、お電話でのお問い合わせは上記とさせていただきます