PlugXと攻撃者グループ "DragonOK"の関連性 | LAC WATCH

By 石川 芳浩

Published: 2017-12-18 · Archived: 2026-04-05 15:13:02 UTC

当社サイバー救急センターの脅威分析チームでは、JPCERT/CCが2017年1月12日の分析だよりで報告※1している Poison IvyのAPI Hashコードを利用したPlugX（以下、PIPX）による標的型攻撃を、2017年10月頃から複数確認しています。今回は、このPIPXを分析する中で見えた、マルウェアを使用する攻撃者グループについて紹介します。PIPXの詳細な機能についての解説は、前述したJPCERT/CCの分析だよりにありますので、そちらをご覧ください。

PIPXの共通点

脅威分析チームで確認できたPIPXにはいくつかの共通点がありました。その一部を説明します。

1. ファイル情報および実行方法

PIPXをドロップ（インストール）する実行ファイルは、図1および図2に示すような、アイコンリソース情報を持つ RAR の自己解凍形式（SFX）を使用します。また、実行ファイルは、3つのファイルで構成されており、DLLサイドローディングの手法を悪用後、正規プロセスである "nslookup.exe"にPIPXのコードをインジェクションし、実行します（図3）。PIPXに内包されるファイルは、攻撃が行われた時期によって少し異なり、2017年10月頃に確認したキャンペーンでは、図2の実線で囲った赤枠の通り"mcoemcpy.exe, mcutil.dll, Mlog.datまたはmcafee.res"の3ファイルで構成されていました。一方、2016年4月頃に確認したPIPXでは、点線で囲った青枠の通り" RasTls.exe, RasTls.dll, RasTls.dll.msc"という3ファイルで構成されていました。

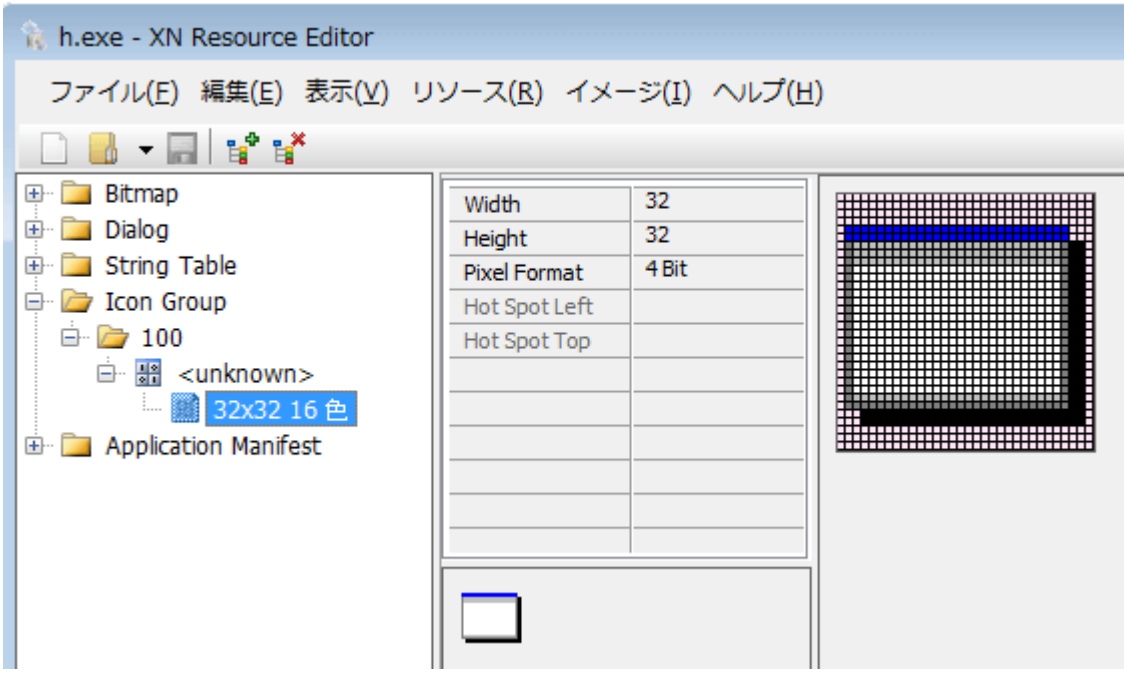
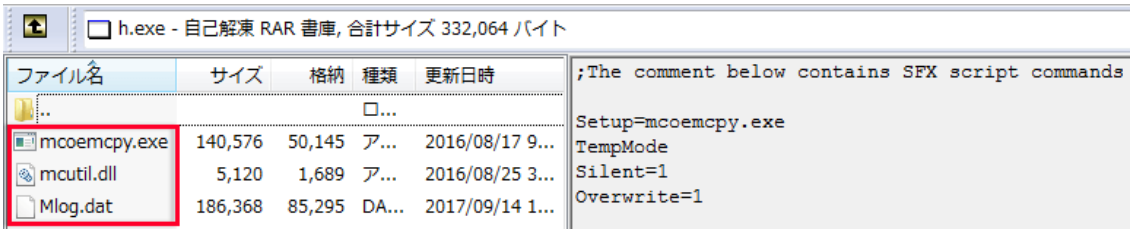


図1 PIPXのアイコンリソース情報



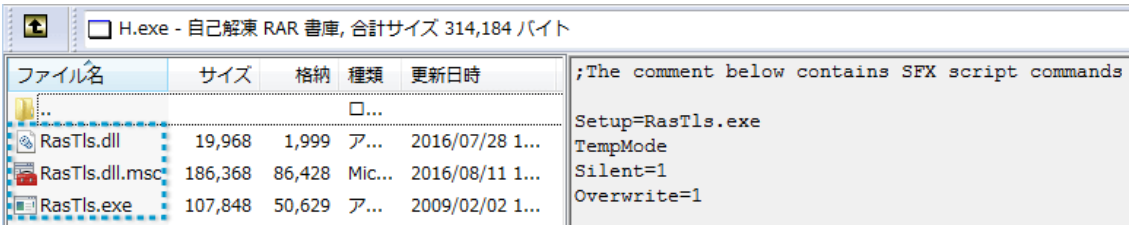


図2 PIPXに内包されるファイル2017年（上）/2016年（下）

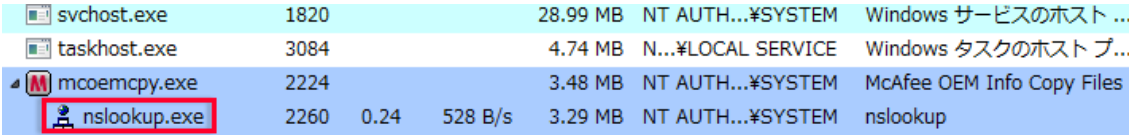
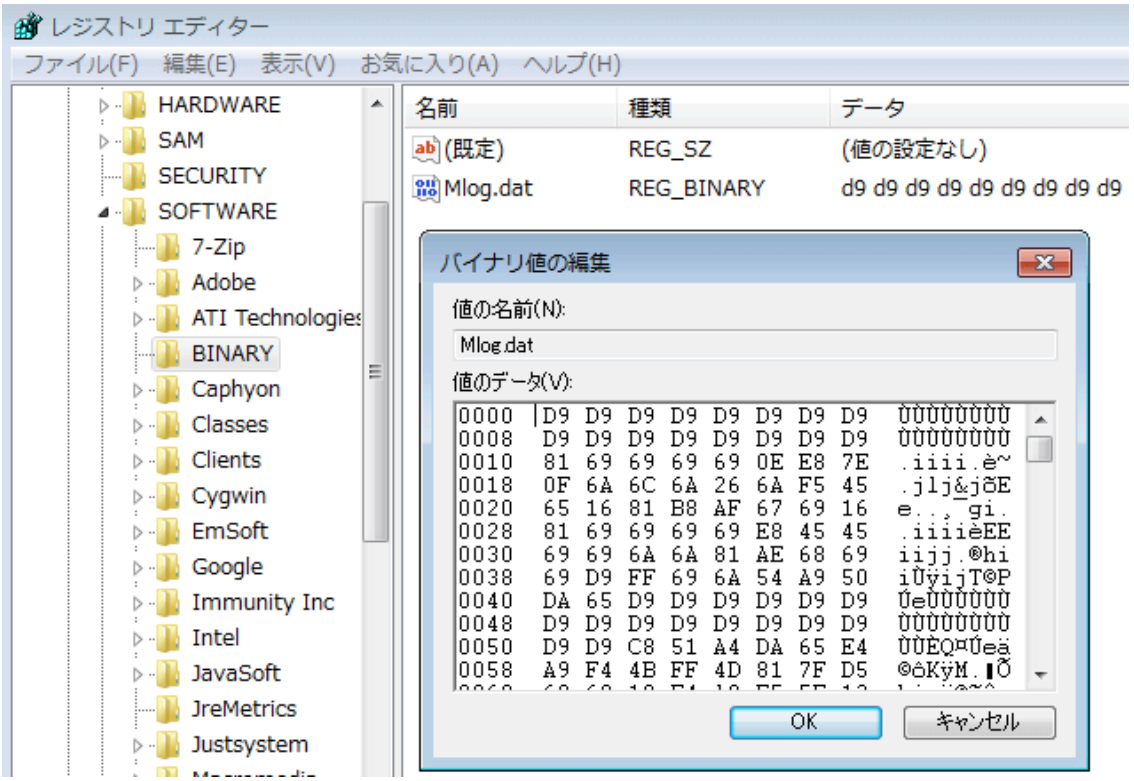


図3 "nslookup.exe" にPIPXのコードをインジェクション

2. 自動実行の仕組み

PIPXは、サービスまたは自動実行のレジストリキー[1]に登録された正規プログラムからDLLサイドローディングの手法を悪用し、自動実行します。その中で、ペイロードに相当する暗号化されたデータは、ファイルとして読み込むのではなく、特定のレジストリキー[2]に格納されたレジストリ値から読み込みます。図4に示すように、レジストリ値のデータとPIPXに内包されたファイルデータが同じであることが確認できます。

- *1* 管理者権限の場合はサービスを利用し、一般ユーザ権限の場合はレジストリキーを利用する
- *2* HKLM\SOFTWARE\BINARY（管理者権限の場合）またはHKCU\SOFTWARE\BINARY（一般ユーザ権限の場合）



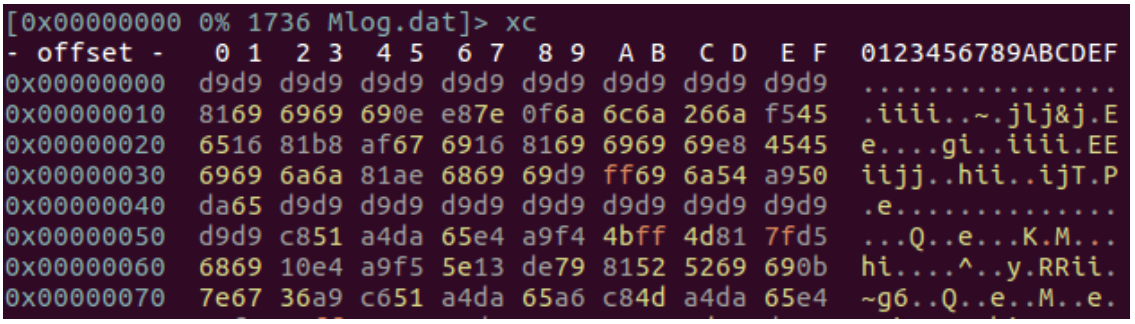


図4 ペイロードデータの比較。レジストリ値（上）/ PIPXに内包されたファイルデータ（下）

3. 設定情報

設定情報のサイズは、0x36a4バイトであり、図5に示すような情報が含まれ、PIPXは、この情報を元に動作します。

```
sub_79502(&dword_87DA4, 0, 0x36A4);
sub_79502(&byte_87DD4, 1, 672);
dword_88FD4 = 0;
dword_87DB8 = 1;
dword_87DA4 = 1;
dword_87DBC = 1;
v0 = sub_606D4(&v17);   インストールフォルダ
sub_66E2C(L"%AUTO%\\emproxy", *(_DWORD *)(v0 + 4));
sub_605ED();
v1 = sub_606D4(&v17);   サービス名
sub_66E2C(L"emproxy", *(_DWORD *)(v1 + 4));
sub_605ED();
v2 = sub_606D4(&v17);   サービス表示名
sub_66E2C(L"emproxy", *(_DWORD *)(v2 + 4));
sub_605ED();
v3 = sub_606D4(&v17);   サービス情報名
sub_66E2C(L"McAfee Email Proxy Service", *(_DWORD *)(v3 + 4));
sub_605ED();
dword_89BDC = 1;
```

```
v12 = sub_606D4(&v17);   スクリーンキャプチャ保存フォルダ名
sub_66E2C(L"%AUTO%\\emproxy\\screen", *(_DWORD *)(v12 + 4));
sub_605ED();
v13 = sub_606D4(&v17);   パスワード
sub_66E2C(L"DMej", *(_DWORD *)(v13 + 4));
sub_605ED();
v14 = sub_606D4(&v17);   Info
sub_66E2C(L"TEST", *(_DWORD *)(v14 + 4));
sub_605ED();
v15 = sub_606D4(&v17);   Mutex
sub_66E2C(L"My_Name", *(_DWORD *)(v15 + 4));
sub_605ED();
```

図5 設定情報（共通部分のコード一部抜粋）

PIPXの通信先

PIPXの通信先に目を向けると、マルウェアの種類やインフラなどの関連要素から"DragonOK"と呼ばれる攻撃者グループによる犯行である可能性が高いことがわかりました。"DragonOK"は、主に日本や台湾などの製造業やハイテク産業などを標的として活動している攻撃者グループであり、FireEyeから公開されたレポート※2によれば、中国の江蘇省を拠点としているとされています。

図6は、PIPXが使用する一部の特徴的な通信先を元に、Maltegoで関連する要素をマッピングしたものです。通信先であるC2サーバのドメイン登録者のメールアドレスは、実線の赤枠で囲った"jack[.]ondo[at]mail[.]com"であることがわかります。このメールアドレスを使用して取得されたドメイン（snoozetime[.]info）は、"Aveo"と呼ばれるマルウェアによって使われていることがPalo Alto Networksによって報告※3されています。さらに関連する要素を調査すると、このドメインに紐づくIPアドレスは、"104.202.173[.]82"であり、このIPアドレスは、ほぼ同時期に点線の青枠で囲ったドメイン

で使用されていたことがわかります。このドメインをC2サーバとして使うマルウェアは、"Sysget"と呼ばれ、"DragonOK"が利用するマルウェアの1つです。このマルウェアは、日本では少なくとも2014年ごろから利用されており、2017年11月下旬の標的型攻撃でも使用されていることを確認しました。機能については、"Sysget v4"※4の亜種に相当するものであると考えられます。

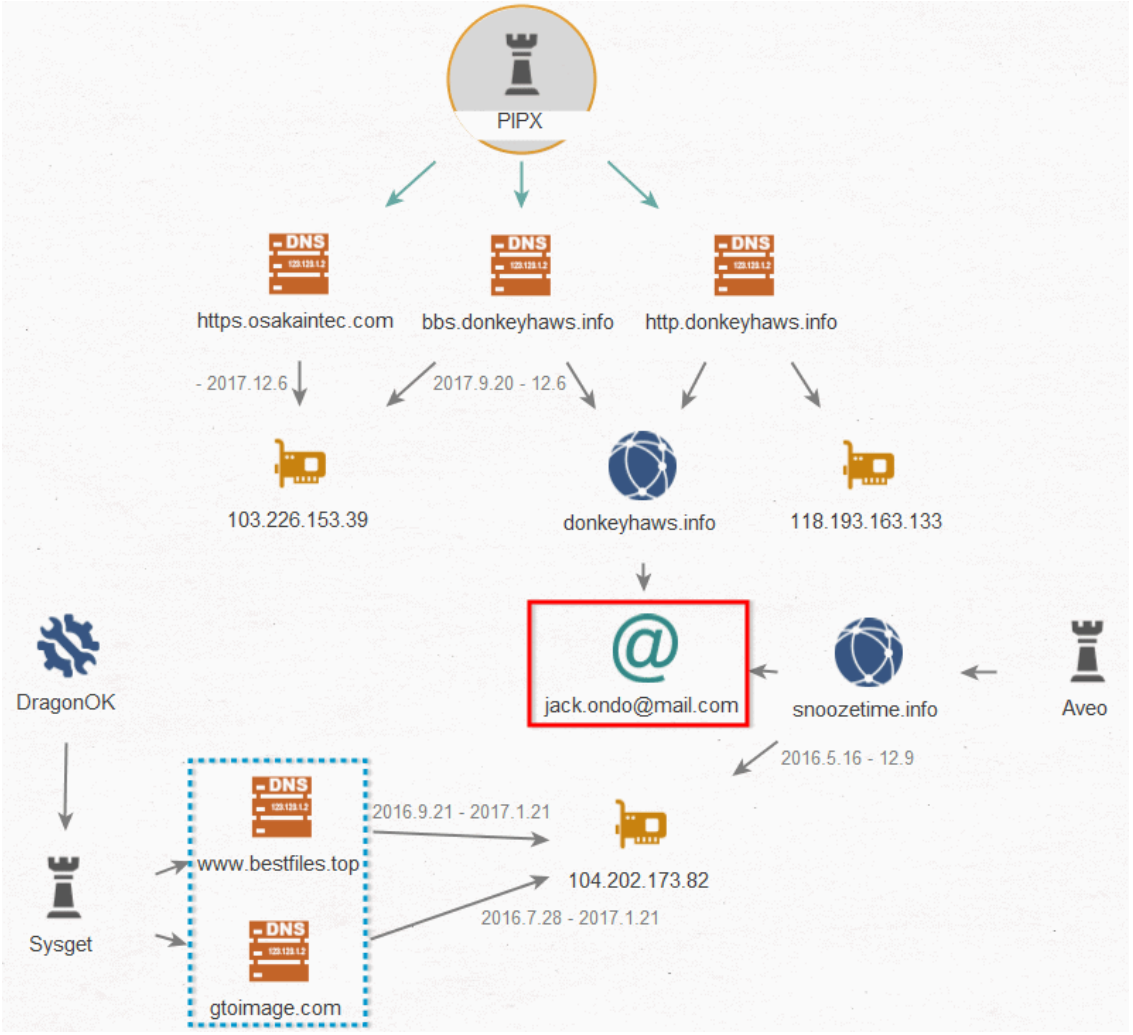


図6 PIPXの通信先と関連性

今後も日本をターゲットにした活動が予想されるDragonOK

日本における"DragonOK"の活動は、2017年に入りほとんど確認できていませんでしたが、2017年10月後半頃から少し大きな動きを確認できました。このことから、"DragonOK"は日本を標的の1つとして絶えず攻撃を仕掛けてきており、今後も日本をターゲットに継続的に活動することが予想できます。当社脅威分析チームでは、この攻撃者グループ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。

IOC (Indicator Of Compromised)

ハッシュ値

97763d25af878d73d19deabe9ea2d564
29cdae7dc2a7f7376a19e4de91b69c98
58ba2c0ed39d5c874a4933677508f5cc

通信先

php[.]marbletemps[.]com
bbs[.]donkeyhaws[.]info
http[.]donkeyhaws[.]info
https[.]osakaintec[.]com
206.161.218[.]49
207.226.137[.]207
118.193.163[.]133
103.226.153[.]39

- ※1　Poison Ivyのコードを取り込んだマルウエアPlugX
- ※2　OPERATION QUANTUM ENTANGLEMENT
  （https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf）
- ※3　Aveo Malware Family Targets Japanese Speaking Users
- ※4　DragonOK Updates Toolset and Targets Multiple Geographic Regions

---