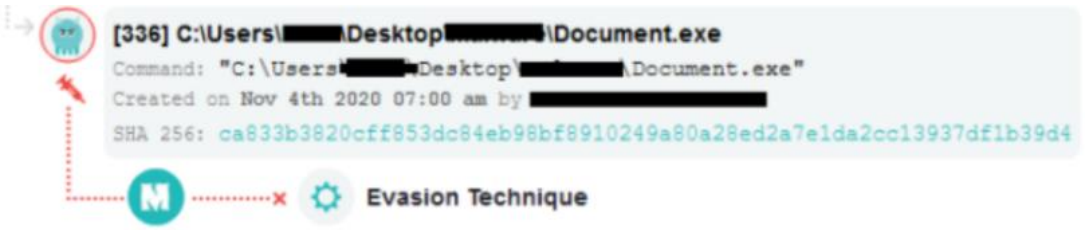

Minerva の敵対的環境攻撃防御手法で BuerLoader を先制防御
2020 年 11 月 18 日 Minerva のブログから

BuerLoader はステルスなローダで、企業組織内のネットワークに攻撃の足掛かりを作るのに最適です。マルウェア感染手法で共通するのはフィッシングメール攻撃で、google ドキュメントリンク先に悪意のあるローダが仕掛けられます。今回ご紹介するのは、攻撃者が AvidXchange というインボイス作成・決済・管理のソリューションで発見しました。通常のフィッシングメールとはまた違った攻撃手法です。

このマルウェアはサンドボックスからのマルウェア検知と旧ソ連邦諸国にあるエンドポイントへ感染させないなどの回避テクニックを行います。初めに NtQueryDefaultLocale 関数を使用し、マシンの居所を判別し、CIS諸国（旧ソ連邦諸国）に属すマシンなどは攻撃から除外されます。

```
NTSTATUS ret = NtQueryDefaultLocale_pointer(0, &lcId);;
if (ret >= 0 || lcId == 0x419 || lcId == 0x422 || lcId == 0x423 || lcId == 0x428 || lcId == 0x43F || lcId == 0x818 || lcId == 0x819)
{
    ExitProcess(0);
}
```

Windowsの API 関数 GetDiskFreeSpaceExA を使いマシンのディスク容量などをチェックします。空き容量が 50GB 以下又は全体容量が 120GB 以下のデバイスであれば攻撃から除外されます。以下は Buer コードが容量をチェックしているスクリーンショットです。

```
if ( !Check_VM_Flag && (v0 < 0 || v0 <= 0 && TotalGBs < 120 || FreeGBs < 50) )
  ExitProcess_1(0);
```

Minerva は BuerLoader を Minerva 敵対的環境攻撃防御モジュールで攻撃の足掛かりとなるマルウェアコードを先制防御しました。

下の図は Minerva ユーザーが実際に攻撃を仕掛けられ先制防御したイベントです。

Minerva 製品(Minerva Armor)についてのお問い合わせは Pico Technologies (info@pico-t.co.jp)までお願い致します。