BlackMatter – ランサムウェアの新ハッカー登場する
2021 年 8 月 31 日 Minerva のブログから

DarkSide ランサムウェアアフィリエイトプログラムが消滅した後、ランサムウェア市場は空洞化と化していました。しかし Lockbit や Black Matter と名乗る新たなグループが強固なランサムウェアを仕掛け始めています。彼らのランサムウェアのいくつかのコードには特徴があり、DarkSide の技術が受け継がれているようです。BlackMatter グループが世の中でほとんど注目されていない最中、Bleeping Computer(コミュニティサイト)によると、このグループは既に 400 万ドルのランサムを稼いていると主張しています。Minerva リサーチチームは最新の BlackMatter グループのランサムウェアサンプルを入手し、ランサムウェアの中枢構造を詳細に調査致しましたので、今回ご紹介します。

回避テクニック:
多くのマルウェアと同様に BlackMatter は暗号化と動的な API 機能解決を繋ぎ合わせて作られていることにより、マルウェア分析を回避して実行します。ランサムウェアの API 解決はエンコードフォームで解決機能ポインターをセーブし、実行時のみデコードされることで特にユニークなマルウェアと言えます。

API 解決機能を非コンパイルされた状態が以下となります。

```
if ( module_handle )
{
  functions_array = (int *)(a1 + 4);
  while ( 1 )
  {
    module_handle = *v4++;
    if ( module_handle == 0xCCCCCCCC )
      break;
    function_from_checksum = get_function_from_checksum(module_handle ^ 0x1002BFFF);
    stub_heap_allocation = RtlAllocateHeap(a3, 0, 16);
    if ( *(_DWORD *)(stub_heap_allocation + 16) != 0xABABABAB )
      *functions_array++ = stub_heap_allocation;
    *(_BYTE *)stub_heap_allocation = -72;
    random_int = w_gen_random(0, 4u);
    if ( random_int )
    {
      switch ( random_int )
      {
        case 1u:
          v13 = w_gen_random(1u, 9u);
          *(_DWORD *)(v14 + 1) = __ROR4__(function_from_checksum, v13);
          *(_WORD *)(v14 + 5) = -16191;
          *(_BYTE *)(v14 + 7) = v13;
          *(_WORD *)(v14 + 8) = -7937;
          break;
```

更なる分析を行うと、マルウェアはヒープ割り当てが整数 0xABABABAB で締めくくると、再構築されたインポートアドレステーブル内にあるスタブのアドレスをセーブしません。この状態でデバッガ時に起動するとランサムウェアは効果的にクラッシュします。このテクニックはヒーププロテクションで防御しています。ヒーププロテクションの詳細については[こちら]。

他にこのグループが使用しているアンチデバッガテクニックというのは、ThreadHideFromDebugger（0x11）パラミターと NtSetInformationThread 機能を使用してスレッドを隠蔽します。よってスレッドがデバッガから回避する要因となります。このテクニックはまさしく Lockbit2.0 グループが使用しているテクニックであると言っても差し支えないことがわかります。 以下は BlackMatter が実際に使用した隠蔽コードスレッドです。

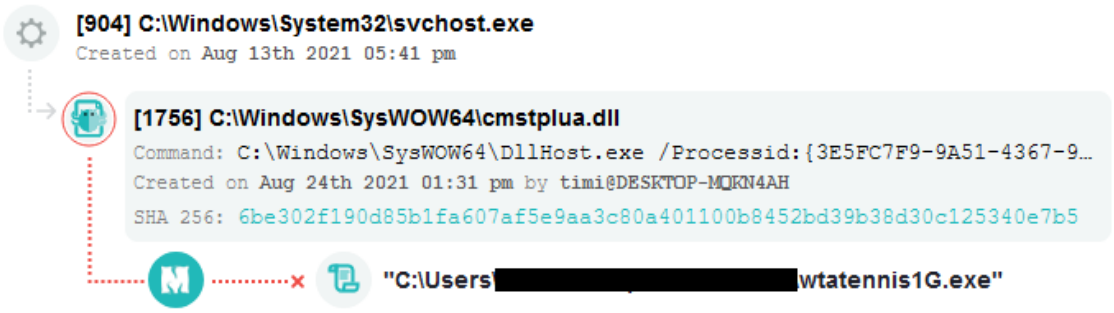
```
signed int v1; // eax

if ( thread_id )
  v1 = thread_id;
else
  v1 = -2;
return NtSetInformationThread_stub(v1, 0x11, 0, 0);
```

他のランサムウェアとは違い、BlackMatter のランサムウェアはロシア製のデバイスも暗号化するでしょう。今回のマルウェアサンプルはコンピューターのローカルをクエリーチェックす

ることなどはせず、サンドボックスや他の場所でもお構いなしに攻撃を行う状態でした。

一般的にランサムウェアはほとんど初期のペイロード攻撃は行いません。なぜならセキュリティ製品が検知され処理されるからです。よって侵入したネットワーク環境を十分に適用するマルウェアでセキュリティ製品から検知回避します。タイプ的にはメモリーインジェクション攻撃又は自給自足型攻撃のような回避型マルウェアと言えるでしょう。Minerva製品は、このようなBlackMatterのランサムウェアが侵入しても、初期ペイロード攻撃前に先制防御します。以下は攻撃防御のタイムラインです。



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。