Monthly Research

実行環境に応じて動作を変えるマルウェアに関する調査

株式会社ＦＦＲＩ
http://www.ffri.jp

Ver 2.00.01

背景：MITBマルウェアによる被害の増加

- オンラインバンキングを狙うMITB（Man-in-the-Browser）マルウェアの被害が増大している
- CitadelなどMITBマルウェアが感染したホストでのみ悪意のある動作する機能[1]を実装していることが確認されている
- 今回、実行環境の検知・識別に注目し、その手法と対策について解説する

なぜ実行環境に応じて動作変えるのか？

- Zeus/SpyEye/CitadelなどのMITBマルウェアはマルウェア開発キットが流通しており、開発キットの開発者とマルウェア運用者が異なる
  - ウィザード形式でマルウェアを作成できる、お手軽な開発キット

- おそらく、１つのマルウェア開発キットで生成されたマルウェアがセキュリティベンダーによって一網打尽にされると困ると推測できる
  - サンドボックスなどを用いた自動解析で振るまいの特徴を捕まえないため、自動解析を識別して動作を変える意図があると推測される
  - また、バイナリが大きく異なれば、同じ開発キットで生成したマルウェアでも亜種として検知できない

実行環境に応じて動作を変えるマルウェアの特徴と動作

- 解析環境を検知し、悪意のある動作を抑制する
  - 採取された後にサンドボックスで実行しても、悪意のある動作をしないため、振る舞いベースの検知で検知されない可能性がある[2]

- 感染したホスト固有の値を実行ファイルに埋め込むマルウェアもある
  - この場合、感染したホスト上のマルウェアはホストごとに違うパターンになるため、従来のシグネチャベースのアンチウィルスでも検知が困難となる

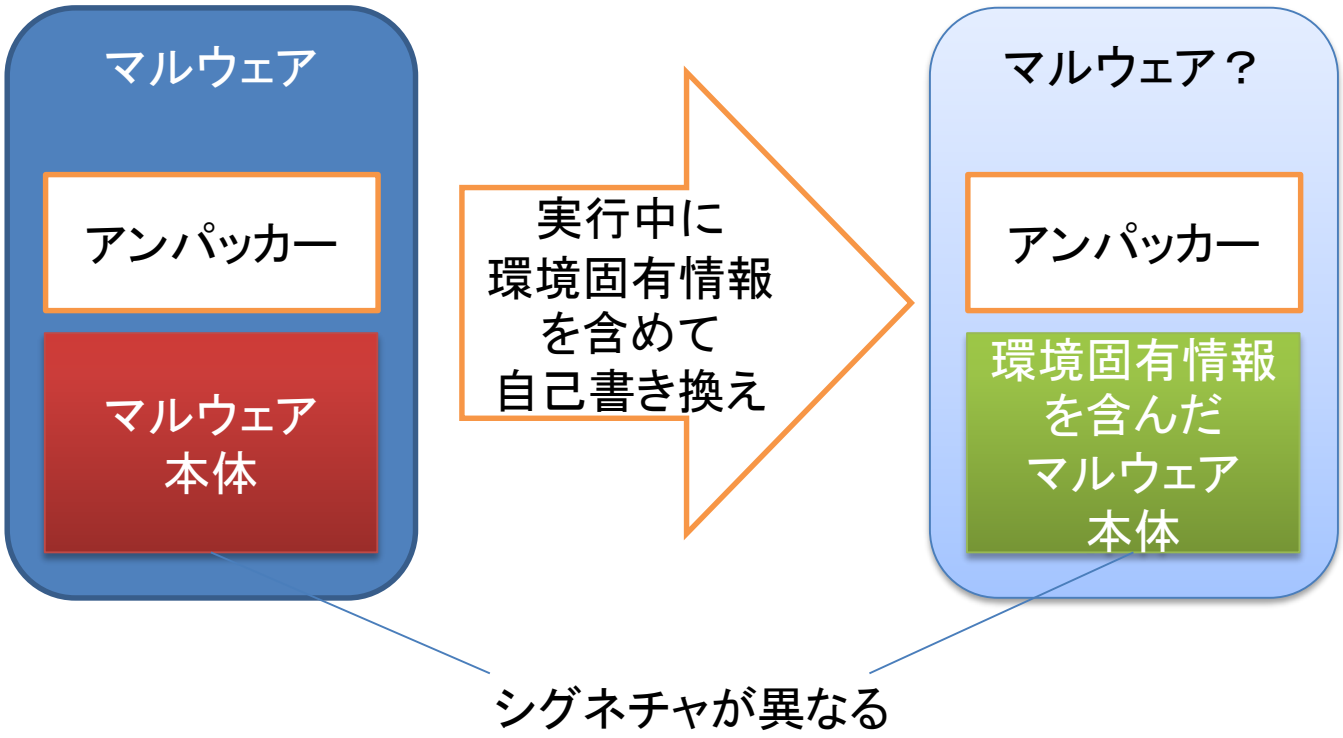
実行環境の検知及び識別に使われるテクニック

- Host fingerprinting
  - ホスト環境固有の情報を使って、感染したホストとそれ以外（自動解析サンドボックスや解析者も含む）を検知し識別する

- 仮想化環境検知
  - 仮想化環境上で実行されているかどうかを検知する

Host Fingerprinting

- 感染したホストの環境固有情報を実行ファイルに埋め込む



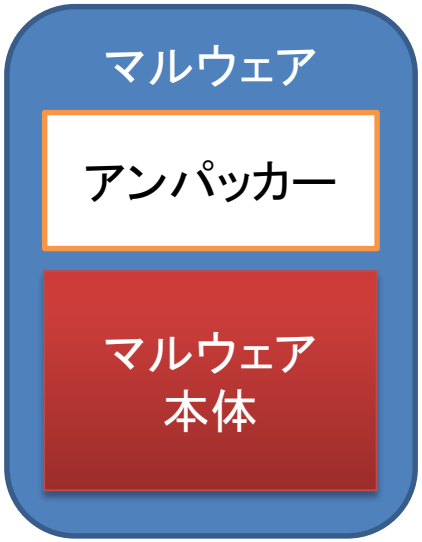
環境固有情報の例

Category	Environment Unique Values
Hardware	**※GUID(Disk)**, MAC address(NIC), etc...
System	OS Product ID, computer(NetBIOS) Name, Registry entry, etc…
Application	**※Execution path**, username, etc…
Network	IP address(external check)

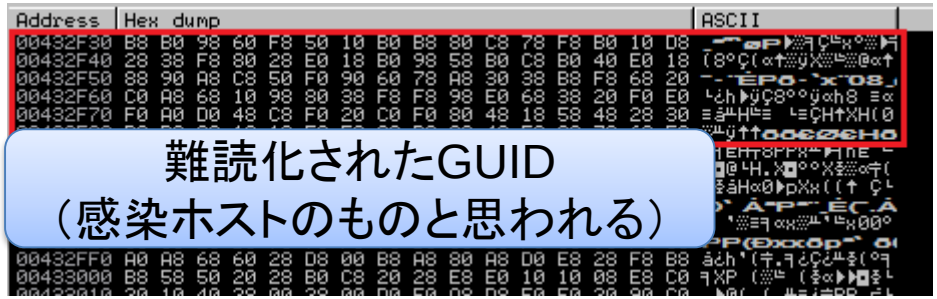
※Citadelマルウェアで使われていることを確認

In real malware

- Citadel系マルウェア(2013年下半期にサンプリング)
  - GetVolumeInformationA()でシステムドライブのGUIDを取得する
  - 環境依存マルウェアは環境依存情報を含んだ自身の実行ファイルをメモリに展開し、取得したGUIDと比較する
  - 一致しなければマルウェアを終了させる



アンパック



環境固有情報が一致しない場合の動作

- 実行を終了する
- 無害なコードを実行し続ける
- 解析者を騙す動作に切り替える
  - ランダムなURLへのネットワークアクセスを試みるなど

※将来的には、パッカーと連携し、環境固有情報を使って実行コードをデコードするようになることも十分にありえる

Host fingerprinting検知・対策

- ヒューリスティック検知におけるルール追加
  - GetVolumeInformation()やGeVolumeNameByHandle() , GetAdaptersAddresses ()など、環境固有情報を取得するAPIを呼ぶ場合、Host fingerprintingを行っている可能性がある

- サンドボックス/自動解析システムでの環境エミュレーション
  - 環境情報を取得するAPIの結果を偽装する

- Symbolic execution[3]
  - 実行ファイル中の条件分岐を網羅するようなテストケースを作成する研究

仮想化環境検知

- マルウェア全体の中で、仮想化環境検知を行なうのは観測されているマルウェアの2%程度(2013年時点） [5]

- 仮想化環境検知の主なアプローチ[4][5][6]
  - 仮想化されたCPU特有の振る舞いにより識別
  - 仮想化ソフトウェア特有のリソースの有無や識別名を探して識別
  - 仮想化されたスクリーンのサイズやサポートするグラフィック機能の有無で検知
  - VMMによるオーバーヘッドあるいはタイミングのズレを用いて検知

- 検知・対策
  - Host fingerprinting検知・対策と同様

まとめ

- 実行環境固有の情報を取得し、その振る舞いを変えるマルウェアによる被害が増えている
- 中でも、特定のホストでしか動作を再現できないHost fingerprintingと呼ばれる手法を使われると、シグネチャマッチングやサンドボックス型自動解析による検知が難しい
- 自動解析を回避するためのもう一つのテクニックとして仮想化環境検知がある
- 環境によって振る舞いを変えるようなマルウェアの解析は、熟練したマルウェア解析エンジニアにとってはさほど問題とならないが、自動解析やシグネチャベースの検知ロジックを回避するには十分
- 自動生成されるマルウェアに効率よく対応するためには、自動解析技術をさらに洗練させていく必要がある

参考文献

- [1]: Analyzing Environment-Aware Malware, Lastline, 2014.05.25(viewed) http://labs.lastline.com/analyzing-environment-aware-malware-a-look-at-zeus-trojan-variant-called-citadel-evading-traditional-sandboxes

- [2]: Martina Lindorfer, Clemens Kolbitsch, and Paolo Milani Comparetti. 2011. Detecting environment-sensitive malware. In *Proceedings of the 14th international conference on Recent Advances in Intrusion Detection* (RAID'11). Springer-Verlag, Berlin, Heidelberg, 338-357. http://dx.doi.org/10.1007/978-3-642-23644-0_18

- [3]: Andreas Moser, Christopher Kruegel, and Engin Kirda. 2007. Exploring Multiple Execution Paths for Malware Analysis. In *Proceedings of the 2007 IEEE Symposium on Security and Privacy* (SP '07). IEEE Computer Society, Washington, DC, USA, 231-245. http://dx.doi.org/10.1109/SP.2007.17

- [4] slabbed-or-not/github , 2014.05.25(viewed) https://github.com/kaniini/slabbed-or-not

- [5]: Aurélien Wailly. Malware vs Virtualization The endless cat and mouse play, 2014.05.25(viewed) http://aurelien.wail.ly/publications/hip-2013-slides.html

- [6]: Kang Li, Xiaoning Li. Comprehensive Virtual Appliance Detection. Black Hat Asia 1014. http://www.blackhat.com/docs/asia-14/materials/Li/Asia-14-Li-Comprehensive-Virtual-Appliance-Detection.pdf

Contact Information

E-Mail ： research—feedback@ffri.jp
Twitter： @FFRI_Research