偽アンチウイルスソフトのスキャン動作時における振る舞いの調査

糟谷　正樹[†1]　河野　健二[†1,†2]

1. はじめに

偽アンチウイルスソフトウェア (Fake AV) は商用のアンチウイルスソフトウェア (Real AV) を模したマルウェアである．Fake AV は，見せかけのファイルスキャンを行い，マルウェアに感染しているという嘘の警告を出す．この警告に騙されたユーザはクレジットカード番号などの個人情報を入力してしまい金銭被害を受ける．Fake AV に感染する具体例の一つとして，Black Hat SEO を利用して不正に Google などの検索結果を釣り上げたウェブページにユーザを誘導して Fake AV の実行ファイルをダウンロードさせる方法がある[1)]．

近年，Fake AV は犯罪者集団が収益を得るために利用しており，その被害は増大しつつある．実際に McAfee の調査[2)] では，ある Fake AV を販売しているサーバを監視したところ，11 ヶ月間で被害総額が 1 億 8000 万ドルを超えたという報告がなされている．また，Kaspersky の調査[3)] によると，ユーザサポート機能を実装している Fake AV が存在すると述べており，本物に近い機能を提供することにより，効率よく収益を上げようとしているといえる．このような背景から Fake AV の対策を行う必要があるといえる．

しかし，現在 Fake AV への対策は十分とはいえない．Rajab ら[4)] や Cova ら[5)] の研究によりシグネチャやブラックリストを利用した対策は，基本的に後追いの対策となるため根本的な解決には至らない．

そこで本研究では Real AV と Fake AV の違いを判断するためにスキャン時のメモリ使用量の変化に着目した．直感的に Real AV はマルウェアをスキャンしたときに多くのメモリを使用し，反対に Fake AV は使用するメモリが少ないと考えられるためである．

この考えを確かめるために，Real AV を 8 個，Fake AV を 38 個収集して，各々に対してマルウェアが存在するときと存在しないときのスキャン時のメモリ使用量のデータを取得した．その結果から Real AV はマルウェアの有無によってメモリ使用量に明らかな違いがあるのに対して，Fake AV では Real AV のような目立った変化が生じなかった．

†1 慶應義塾大学理工学部情報工学科
†2 科学技術振興機構 CREST

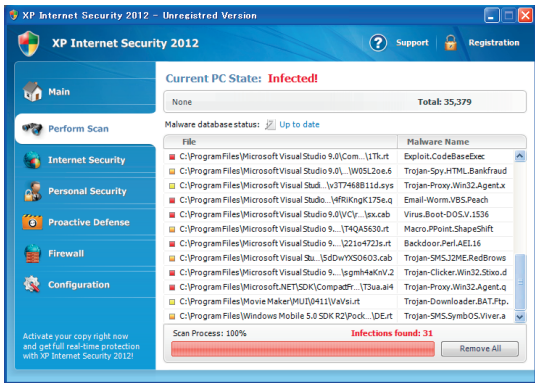

図 1　Fake AV のサンプル

2. Fake AV の振る舞い

Fake AV はユーザを騙すために，あたかも Real AV が提供するようなスキャンを行う．**図 1** は実在する Fake AV のサンプルであり，あたかもマルウェアを検出したかのように表示をしている．しかし，この検出結果は全て偽物である．実際に図 1 の Fake AV は感染した環境上の個々のファイルにアクセスしておらず，ディレクトリにアクセスするのみである．このことから Fake AV がスキャンを行う理由は，ユーザの環境に存在するディレクトリ名を用いて本物らしいスキャン結果を表示するためと推測できる．

また，Fake AV はスキャンに要する時間が Real AV に比べて非常に少ない．これはマルウェアファイルをスキャンするときに行うパターンマッチングやエミュレーションの動作を行わないためと考えられる．

3. 着目点

本研究ではマルウェアの有無によって生じる Real AV と Fake AV のスキャン時におけるメモリ使用量の変化に着目する．Fake AV のスキャン時間が短いのは Real AV と比べて十分な機能を提供していない

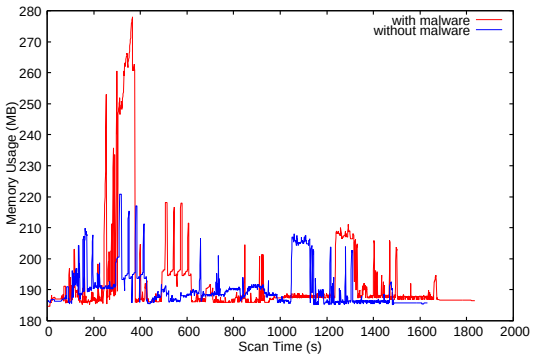

図 2 ある Real AV のスキャン時におけるマルウェアの有無によるメモリ使用量の違い

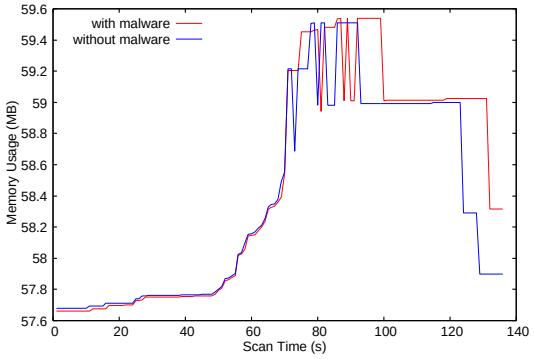

図 3 ある Fake AV のスキャン時におけるマルウェアの有無によるメモリ使用量の違い

ためといえる．そのため，Real AV ではメモリ使用量に明らかな差が生じ，Fake AV ではその差はほとんどないと推測できる．

4. 実　　験

Real AV と Fake AV のスキャン時におけるメモリ使用量の違いを確かめるために，Norton や Kaspersky などのよく利用されている Real AV を 8 個，Fake AV をマルウェア収集サイト[6),7)] やインターネット上から 38 個集めた．各々のアンチウイルスソフトがインストールされている環境に，合計約 500 MB の様々なタイプのマルウェアを配置したときと配置しなかったときのメモリ使用量の違いを調べた．実験環境は使用 OS が Windows XP SP3 on VMware Fusion 3.1.3, CPU が Quad-Core Intel Xeon 2.4 GHz，SSD を 80 GB 割り当て，搭載メモリが 2 GB である．

Real AV はマルウェアが実験環境上にある場合に，メモリを多く消費していることが**図 2** の 200 秒から 400 秒の部分から読み取ることができる．他の Real AV も図 2 のようにマルウェアがあるときはメモリ使用量が明らかに変化した．一方，Fake AV では，マルウェアの有無によってメモリ消費量に著しい変化がないことが**図 3** のグラフから読み取ることができる．同様に，他の Fake AV も図 3 のようにマルウェアの有無によりスキャン時にメモリ使用量に目立った違いが表れなかった．しかし，一部の Fake AV ではマルウェアの有無によらずメモリ使用量がきまぐれに変わるものが存在した．これらの Fake AV に対してどのように分類を行うか議論していく必要がある．

5. まとめと今後の課題

Real AV と Fake AV はマルウェアのスキャン時にメモリ使用量に違いが出ることが分かった．Real AV はマルウェアをスキャンする際に多くのメモリを利用するのに対して，Fake AV はマルウェアの有無によってメモリ使用量が変化しない．今後の課題として両者の差が統計的に違うことを示すこと，気まぐれにメモリ使用量が変わる Fake AV に対処することである．

参　考　文　献

1) Wang, D. Y., Savage, S. and Voelker, G. M.: Cloak and Dagger: Dynamics of Web Search Cloaking, *Proceedings of the 18th ACM conference on Computer and communications security (CCS '11)*, pp.477–489 (2011).
2) Paget, F.: Running Scared: Fake Security Software Rakes in Money Around the World, http://www.mcafee.com/us/resources/white-papers/wp-running-scared-fake-security-software.pdf (2010).
3) Brulez, N.: Technical Support – they're not always the good guys, http://www.securelist.com/en/blog/249/Technical_Support_theyre_not_always_the_good_guys (2010).
4) Rajab, M. A., Ballard, L., Mavrommatis, P., Provos, N. and Zhao, X.: The Nocebo Effect on the Web: An Analysis of Fake Anti-Virus Distribution, *Proceedings of the 3rd USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '10)* (2010).
5) Cova, M., Leita, C., Thonnard, O., Keromytis, A.D. and Dacier, M.: An Analysis of Rogue AV Campaigns, *Proceedings of the 13th International Symposium on Recent Advances in Intrusion Detection (RAID '10)*, pp.442–463 (2010).
6) Offensive Computing: Offensive Computing ; Community Malicious code researh and analysis, http://offensivecomputing.net.
7) Malware Domain List: http://www.malwaredomainlist.com/.