[Work in Progress] 研究報告

利用者の活動を考慮したHTTPのログ解析によるウィルス通信検出の試み

東　悠樹[1]　鳩野逸生[2,a)]

Attempt to Detect HTTP Traffic by Virus Based on HTTP Log Analysis That Takes into Account User's Activity

近年、コンピュータウイルスに代表されるマルウェアが巧妙化し，アンチウイルスソフトウェアだけでは感染を防止することが困難な状況になって来ており，運用管理者は組織内の PC がマルウェアに感染することを前提とした対策を取ることが求められている．

マルウェアが情報の漏洩や遠隔操作される場合には、マルウェアは外部との通信に HTTP 通信を用いることが多い．本報告では，神戸大学をはじめとする多くの組織で取得・保存されている HTTP 通信ログを用いて，マルウェアに感染した組織内の PC を特定することを試みる．HTTP 通信ログには，送受信元，URL, referer, User-Agent などの情報が含まれており，マルウェアの特定に利用できることが期待できる．

各 PC から発生する HTTP 通信は，PC ユーザが Web ブラウザを操作することに発生するものと，ソフトウェアの更新等のためにバックグラウンドで動作するプログラムが発生するものが含まれている．PC ユーザが Web ブラウザを操作することにより発生する通信は，マルウェアによるものとは考えられない．そのため，利用者による通信の特定にあたっては，事前調査の結果判明した 12 時から 13 時の間にピークを持つ通信に含まれる User-Agent 情報を持つ通信をユーザ操作によるものだとみなし，その通信に含まれる通信先ドメイン，およびそのドメインが referer に含まれる通信先を安全な通信先とみなす．判定にあたっては，各 PC からの通信を，1 時間毎に分割し，各時間帯における行数のカウントを通信に含まれる User-Agent 毎に実施する．

以上の操作によって除かれた通信以外の中から，Windows Update のような正当なソフトウェアの更新によるものを除いたものをリスト化して，Virus チェックサイト Virustoal[1] により悪性のものである可能性があるかチェックを行う．

表 1　危険と考えられるドメイン先と、そのドメイン先と通信を行っている PC の台数

domain	Number of Source IP
DSitePro ○○	8
toptools ○○	7
newnext. ○○	6
backupgr ○○	6
info-str ○○	6
databssi ○○	5
mobogeni ○○	3
slimware ○○	3

本報告における手法を, 神戸大学に保存されている HTTP 通信ログ (2014 年 11 月 1 日–2015 年 10 月 31 日) に適用を試みた．その結果を表 1 にマルウェアの通信先であると考えられるドメインと、そのドメインと通信を行っている PC の台数が多かったものをログを探すことにより検出した結果を示す。

本報告で述べた手法には,

- ユーザによる通信特定に用いた発見的知識は，利用者の業務・活動形態が異なっている場合は適用できない可能性がある．
- 実際のウィルスの挙動を見ると、定期的に通信を行っているものもあるが、ある時点でまとめて外部に情報を漏洩しているケースも存在している．

のような場合には，感染 PC の検知精度が大きく落ちると思われる．今後は，利用パターンを統計的に分析して，変化がないかを継続的にチェックすることによりマルウェアの感染を検知することができないか等を検討していく必要がある．これには，ディープラーニングなどの機械学習手法の応用が期待できる．

参考文献

[1]　Virustotal, https://www.virustotal.com/

[1] 神戸大学大学院システム情報学研究科
Nada, Kobe, 657–8501, Japan
[2] 神戸大学情報基盤センター
Nada, Kobe, 657-8501, Japan
[a)] hatono@kobe-u.ac.jp