マルウェア対策ユーザサポートシステムを用いた CCC DATASet 2011 検体の自動検知と駆除

川口 信隆[*1] 余田 貴幸[*1] 山口 演己[*1] 寺田 真敏[*1]
笠木 敏彦[*2] 星澤 裕二[*3] 衛藤 将史[*4] 井上 大介[*4] 中尾 康二[*2, 4]

[*1] 株式会社日立製作所 神奈川県横浜市戸塚区吉田町 292 番地 nobutaka.kawaguchi.ue@hitachi.com

[*2]KDDI 株式会社 東京都千代田区飯田橋 3-10-10

[*3] 株式会社セキュアブレイン 東京都千代田区麹町 2-6-7

[*4] 独立行政法人情報通信研究機構 東京都小金井市貫井北町 4-2-1

あらまし 我々は，ユーザPC上で動作する不審プログラムをマルウェア動的解析システムで解析し，検知されたマルウェアを自動駆除する「マルウェア対策ユーザサポートシステム」の研究開発を行っている．本システムは，動的解析システムが生成する挙動解析レポートを基に，駆除ツールを作成し，実行することで，マルウェア本体の駆除に加えて，マルウェアが作成・改ざんしたファイルやレジストリ等の削除・修復を実現する．本稿では，本システムの概要について述べるとともに、本システムを用いたCCC DATASet 2011検体の検知・駆除実験について述べる．

Automatic Detection and Removal of Malware in CCC DATASet 2011 using Anti-Malware User Support System

Nobutaka Kawaguchi[*1] Takayuki Yoda[*1] Hiroki Yamaguchi[*1] Masato Terada[*1]
Toshihiko Kasagi[*2] Yuji Hoshizawa[*3] Masashi Eto[*4] Daisuke Inoue[*4] Koji Nakao[*4]

[*1]Hitachi, Ltd.: 292 Yoshida-Cho Totsuka-Ku Yokohama, Kanagawa, Kanagawa nobutaka.kawaguchi.ue@hitachi.com

[*2]KDDI Corporation: 3-10-10 Iidabashi Chiyoda-Ku Tokyo

[*3]SecureBrain Corporation: 2-6-7 Koji-Machi Chiyoda-Ku Tokyo

[*4]National Institute of Information and Communication Technology: 4-2-1 Nukui-Kitamachi, Koganei Tokyo

Abstract The authors have been developing Anti-Malware User Support System, which analyzes suspicious programs installed on users' PCs by employing dynamic malware analysis systems and automatically removes detected malicious programs. In addition to removing the malicious programs, this system can remove/repair files and registries that the malicious programs created/modified by generating removal tools based on behavior analysis reports obtained from the dynamic malware analysis systems. In this paper, we will show how this system analyzes and removes malware in CCC DATASet 2011.

1 はじめに

今日，日々数千から数万の新種マルウェアが出現している．これに伴い，シグニチャファイルを基にユーザPC内からウイルスを検知するアンチウイルスソフトは，シグニチャファイルの更新頻度が新種マルウェアの出現速度に間に合わず，検知率が低下している．

この問題を解決するために，我々は，シグニチャに依存せずにマルウェアを検知・駆除する「マルウェア対策ユーザサポートシステム」の研究開発を進めている[1]．本システムは，ユーザ

PC にインストールされた，不審な実行ファイル（擬陽性ファイル）を，マルウェア動的解析システム[2-3]を用いて解析する．解析の結果，マルウェアが検知された場合，本システムは，駆除ツールを自動生成し，マルウェアを駆除する．

動的解析システムは，プログラムを計算機上で実行し，その挙動（ファイルアクセスやネットワーク通信など）を基にマルウェア判定を行うため，シグニチャファイルが対応しない，未知のマルウェアを検知できる．また，動的解析システムが提供する，挙動解析結果レポートを利用することで，マルウェア本体に加えて，マルウェアが生成・改ざんした，ファイル・レジストリ等を駆除する，駆除ツールを生成することができる．

本稿では，本システムを用いた CCC DATASet 2011 検体の検知・駆除実験について報告する．特に，挙動解析結果レポートに基づいて生成された駆除ツールが，マルウェアが PC に及ぼした改ざんを，どの程度修復できたかについて述べる．

以下，第 2 章では，本システムの概要について述べる．第 3 章では，挙動解析結果レポートに基づく，駆除ツールの生成方法について詳説する．第 4 章では，CCC DATASet 2011 検体を用いた検知・駆除実験の結果について述べる．第 5 章を本論文のまとめとする．

2 システムの概要

図1に，マルウェア対策ユーザサポートシステムの概要を示す．ユーザ PC で発見された擬陽性ファイルは，ネットワークを介してユーザサポートセンタに送信され，マルウェア動的解析システムで解析される．ファイルがマルウェアと判定された場合は，駆除ツールが配信される．

本システムは，以下の 6 種類のモジュールから構成される．

1. 検査ツール
   ユーザ PC 内に常駐し，擬陽性ファイルを発見する（図 1(1)）．具体的には，新規プロセスが起動する度に，実行ファイルを静的解析し，不審なセクションや IAT(Import Address Table)がある場合に，擬陽性ファイルと判断する．マルウェアを漏れなくマルウェア動的解析ステムで解析するために，僅かでも不審な特徴があるファイルは，擬陽性ファイルに分類する．
2. クライアントエージェント（CA）
   サーバエージェントに擬陽性ファイルを送信する（図 1(2)）．また，ファイルがマルウェアの場合は，駆除ツールを受け取り，実行する（図 1(6)）．
3. サーバエージェント(SA)
   後述のホワイトリストフィルタ，駆除ツール生成システム，マルウェア動的解析システムと連携し，CA から受信した擬陽性ファイルがマルウェアの場合に，駆除ツールを配信する（図 1(2)-(6)）．
4. ホワイトリストフィルタ
   ホワイトリストフィルタには，既知の非マルウェア（正規アプリケーション）のハッシュ値が登録されおり，受信した擬陽性ファイルが，既知の非マルウェアであるか否かをチェックする（図 1(3)）．ファイルが既知の非マルウェアの場合は，以降の処理（図 1(4)-(6)）は行われない．本システムのプロトタイプ実装では，約800万件の正規Windowsプログラムのハッシュ値が登録されている．
5. マルウェア動的解析システム
   既知の非マルウェアではないファイルを解析し，挙動解析結果レポートを生成する（図 1(4)）．レポートには，マルウェア判定結果及び，ファイルの挙動情報が載っている．SA は，擬陽性ファイルと共に，ユーザ PC の環境情報（OS 等）を，動的解析システムに送信する．動的解析システムは，ユーザ PC に最も近い環境で解析をすることで，マルウェアがユーザ PC 上でどういった活動を行ったかを正確に知ることが出来る．本システムのプロトタイプ実装では，NICT が研究開発している，nicter ミクロ解析システム（以下，nicter）[2]を用いている．nicter は，Windows XP/Vista/7 の解析環境を備えている．
   尚，次章で述べるとおり，SA は，受信した挙動解析結果レポートを，共通解析結果レポ

ートに変換する.

6. 駆除ツール生成システム
   SA から受信した共通解析結果レポートを基に, 駆除ツールを生成する(図 1(5)). 尚, 次章で述べるとおり, 駆除ツールは, エンジン部とパターンファイルから構成され, 駆除ツール生成システムでは, パターンファイルを生成する.

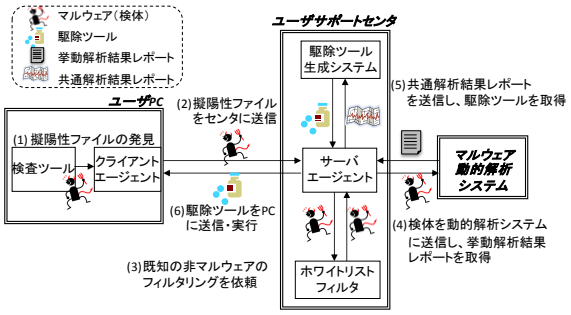

図 1 ユーザサポートシステムの概要

3 駆除ツールの生成

本章では, 駆除ツールの生成方法について述べる. 先述のとおり, 駆除ツールは, パターンファイルとエンジン部から構成される. パターンファイルには, マルウェアをユーザ PC から駆除するのに必要な手順が記されている. パターンファイルは, 共通解析結果レポートを基に, 駆除ツール生成システムが作成する. 一方, エンジン部は実行ファイルであり, パターンファイルに従って, 駆除処理を行う. エンジン部は, ユーザ PC に予めインストールされている. 以下に, 共通解析結果レポート及び, パターンファイルの詳細について述べる.

3.1 共通解析結果レポート

動的解析システムによって, 挙動解析結果レポートの形式は異なる[4]. このため, SA は, 駆除ツール生成システムにレポートを送信する前に, レポートを共通形式に変換する. 共通形式に変換されたレポートを, 共通解析結果レポートと呼ぶ. レポートは XML 形式である. 図 2 に, レポートの概要を示す.

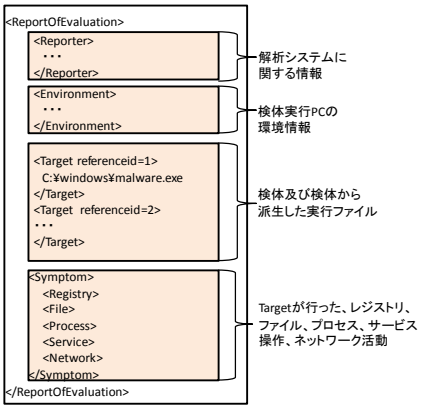

図 2 共通解析結果レポート

Reporter 要素には解析システムに関する情報が, Environment 要素にはマルウェアが実行された解析環境の情報が記載される.

Target 要素には, 検体及び, 検体から派生した実行ファイルのファイル名やハッシュ値, 実行ファイルがマルウェアであるか否かの判定情報が記載される. 特に, 検体に対応した Target 要素には, 検体のユーザ PC 上でのファイルパスが originalfilepath 属性に記載される.

1つ以上の Target 要素がマルウェアと判断された場合に, 共通解析結果レポートは駆除ツール生成システムに送信される.

検体の挙動に関する情報は, Symptom 要素内の, Registry 要素, File 要素, Process 要素, Service 要素, Network 要素に記載される. Registry 要素には, レジストリの追加や削除, File 要素には, ファイルの作成や追記・削除, Process 要素にはプロセスの起動や停止, Service 要素にはサービスの登録・削除・起動・停止, Network 要素には外部端末との通信内容が記載される.

3.2 パターンファイル

駆除ツール生成システムは, 入力として与えられた共通解析結果レポートの内容を分析し, パターンファイルを作成する.

パターンファイルは複数行のマクロコマンドから構成される. マクロコマンドは, マルウェアをユーザ PC から駆除するための処理を指定する. 表 1 に主なマクロコマンドを示す.

表 1 マクロコマンド一覧

マクロコマンド	説明
DELFILE filepath	filepath で指定されたファイルを PC から削除する．削除対象のファイルが実行中の場合，プロセスを停止した後に，削除を行う．
DELLINE filepath data	filepath で指定されたテキストファイルからテキストデータ data を削除する．
DELREG registry	registry で指定されたレジストリを削除する．
DELPATHSPECFROMREG registry	registry で指定されたレジストリの値を，デフォルト値に戻す．
TERMINATE processpath	processpath で指定されたファイルのプロセスを停止する．
STARTSERVICE servicepath	servicepath で指定されたサービスを開始する．
STOPSERVICE servicepath	servicepath で指定されたサービスを停止する．
DELHASH hashvalue	PC をスキャンし，hashvalue で指定されたハッシュ値を持つファイルを削除する．
DELSIG signature	PC をスキャンし，signature で指定されたウイルスに感染したファイルから，ウイルスを削除する．

パターンファイルには先ず，マルウェア本体を削除するために，共通解析結果レポートの各 Target 属性の originalfilepath 属性を引数とする DELFILE コマンドが記述される．

Registry 要素に関しては，マルウェアが，PC 起動時に自動実行するプログラムを設定する Run キーを作成した場合は，DELREG コマンドを記述する．マルウェアが，各ファイル拡張子の規定アプリケーションを指定するキーを改ざんした場合は，DELPATHSPECFROMREG コマンドを記述する．

File 要素に対しては，マルウェアがファイルを削除した場合は DELFILE コマンドを，テキストファイルの内容を改ざんした場合は DELLINE コマンドを記述する．

Process 要素に対しては，マルウェアが新規プロセスを起動した場合は，TERMINATE コマンドを記述する．

Service 要素に対しては，マルウェアがサービスを起動した場合は STARTSERVICE コマンドを，実行中のサービスを停止した場合は，STOPSERVICE コマンドを記述する．

その他，マルウェアが自己変貌型(ファイル名やデータ構造が異なるコピーを作成する)[1]である場合は，DELHASH コマンドを記述する．また，マルウェアが，他ファイルに感染するウイルスタイプのものである場合は，DELSIG コマンドを記述する．

4 CCC DATASet 2011 検体の検知と駆除

本章では，ユーザサポートシステムのプロトタイプ実装を用いた，CCC DATASet 2011 検体の検知・駆除実験の結果について述べる．

4.1 実験環境

実験は，ユーザ PC，SA，ホワイトリストフィルタ，駆除ツール生成システム nicter が接続されている 100 Mbps LAN 上で行った．ユーザ PC は VirtualBox の仮想マシンであり，OS は Windows 7 SP0 である．SA と駆除ツール生成システムは，VMWare VSphere の仮想マシンであり，OS は Centos5.4 である．ホワイトリストフィルタは VMWare VSphere の仮想マシンであり，OS は Windows 2003 Server である．

4.2 実験対象検体

表 2 に実験対象の検体を示す．nicter が検知可能な CCC DATASet 2011 検体のうち，違うファミリーに属し，ファイルアクセスパターンの特徴が異なる 3 つの検体を実験対象とした．

表 2 実験対象検体

#	SHA1 ハッシュ値	ファミリー(MS Security Essentials)
A	0x5C119…	Trojan:Win32/Ircbrute
B	0x5E2D7…	VirTool:Win32/DelfInject.getn!BI
C	0x6AA8B…	Trojan:Win32/Siscron

4.3 実験方法

検体をユーザ PC 上で起動し，サポートセンタから配信される駆除ツールの駆除性能を評価した．また，検体を起動してから駆除ツールが配信されるまでにかかる時間を測定した．尚、ファイアーウォールを設置し，マルウェアのトラヒックがインターネットに流出しないようにした．

表 3 検体が作成したファイル・レジストリとパターンファイルの比較

#	パターンファイルの主な記述	ユーザ PC 上に作成された主なファイル・レジストリ
A	DELFILE C:¥Users¥TestUser¥malware_sample¥検体 A.exe TERMINATE C:¥Users¥TestUser¥malware_sample¥検体 A.exe DELFILE c:¥RECYCLER¥R-1-5-21-･･･¥Desktop.ini DELFILE c:¥RECYCLER¥R-1-5-21-･･･¥acleaner.exe	C:¥RECYCLER¥R-1-5-21-･･･¥Desktop.ini C:¥RECYCLER¥R-1-5-21-･･･¥acleaner.exe
B	(検体 B のパターンファイル) DELFILE C:¥Users¥TestUser¥malware_sample¥検体 B.exe TERMINATE C:¥Users¥TestUser¥malware_sample¥検体 B.exe TERMINATE C:¥Users¥%USERNAME%¥AppData¥ Roaming¥Reader_sl.exe DELREG HKLM¥Software¥Microsoft¥Windows¥CurrentVersion¥Run,patches DELREG HKU¥Software¥Microsoft¥Windows¥CurrentVersion¥Run, Adobe Reader Speed Launchers DELREG HKLM¥Software¥Microsoft¥Windows¥CurrentVersion¥Run, Adobe Reader Speed Launchers	C:¥Users¥TestUser¥AppData¥Roaming¥Reader_sl.exe HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run¥patches HKU¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run ¥Adobe Reader Speed Launchers HKLM¥Software¥Microsoft¥Windows¥CurrentVersion¥Run ¥Adobe Reader Speed Launchers
C	(検体 C のパターンファイル) DELFILE C:¥Users¥TestUser¥検体 C.exe DELFILE C:¥Users¥TestUser¥検体 C.nls DELFILE %Systemroot%¥System32¥advapi32.exe DELFILE %Systemroot%¥System32¥advapi32.nls TERMINATE %Systemroot%¥System32¥advapi32.exe DELREG HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run,smwcore (acrproxy.exe のパターンファイル) DELFILE c:¥windows¥system32¥acproxy.exe DELFILE c:¥windows¥system32¥acproxy.nls DELFILE %Systemroot%¥System32¥adst.exe DELFILE %Systemroot%¥System32¥adst.nls TERMINATE %Systemroot%¥System32¥adst.nls DELREG HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run,smwcore	C:¥Windows¥System32¥acproxy.exe C:¥Windows¥System32¥acproxy.nls HKU¥Software¥Microsoft¥Windows¥CurrentVersion¥Internet Settings¥Connections ¥SavedLegacySettings HKU¥Software¥Microsoft¥windows¥CurrentVersion¥Internet Settings¥ProxyEnable HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run¥smwcore

4.4 実験結果

4.4.1 駆除性能

表 3 に，駆除ツール生成システムが生成した，各検体のパターンファイル及び，各検体がユーザ PC に作成したファイル・レジストリを示す．各パターンファイルの最上位行には，検体本体を駆除するコマンドが記述され，以下，検体が作成したファイル・レジストリを駆除するためのコマンドが続く．

検体 A は起動すると，リサイクルフォルダ内に自身のコピーと設定ファイルを作成する．ファイルパスは不変（実行タイミングにより変わらない）であるため，nicter の解析結果に基づくパターンファイルに従い駆除処理を行うことで，マルウェア本体及びマルウェアが作成したファイルを全て駆除できる．

検体 B は起動すると，ユーザディレクトリ内に自身のコピーを作成し，起動する．検体 B はその後，コピーの Run キー登録を行う．コピーのファイルパス及びレジストリパスは不変であるため，検体 B のパターンファイルによって，マルウェア本体とそのコピー，及び Run キーを全て駆除することができる．

検体 C は，検体 B と同様に，システムディレクトリ内に自身のコピー及び関連ファイルを作成して起動すると共に，Run キーにコピーを登録する．しかし，検体 B と異なり，コピーのファイル名は，実行のタイミングにより変化する．表 3 では，ユーザ PC では，コピーファイル名は acproxy.exe となるが，nicter では，advapi32.exe となっている．このため，検体 C のパターンファイルでは，acproxy.exe 及びその関連ファイルの駆除に失敗する．

しかし，acproxy.exe が起動すると，サポートセンタに送信されマルウェアと判定されるため，パターンファイルが作成される．このパターンファイルを実行することで，acproxy.exe 及びその関連ファイルを駆除することができる．

4.4.2 処理性能

表 4 に，検体の検知・駆除処理時間を示す．検体 A の処理時間は 3 分程度であり，検体 B・C の処理時間は 10 分程度となっている．検体 A と検体 B・C で処理時間が大きく異なるのは，検体が Run キー登録を行う場合，nicter が解析環境を再起動し，もう 1 度検体を解析するためであ

る. また, 駆除ツールのパターンファイルの生成にかかる時間は, 何れの検体でも数秒程度であり, 他の処理と比べて, 短い時間になっている.

表 4 検体の検知・駆除処理時間

処理内容	検体 A	検体 B	検体 C
検体解析	132	528	544
パターンファイル生成	5	6	3
駆除ツール配信・実行	17	3	18
その他	34	117	43
合計	188	654	608

単位: (秒)

4.4.3 考察

4.4.1 で述べたとおり, 本システムでは, マルウェアが作成するファイルパスが不変である場合は, マルウェア本体の解析結果を基に, ファイルを全て駆除することが可能である. また, ファイルパスが不変ではない場合であっても, 作成されるファイルの種類が実行ファイルの場合は, 最終的に駆除することが可能である. マルウェアを構成するファイルのうち, 最も有害なものは実行ファイルであるため, 本システムにより, マルウェア脅威の大部分を無害化することが可能と言える.

また, 4.4.2 で述べたとおり, 本システムでは, マルウェアの検知・駆除を, 最大 10 分程度で完了する. 一般的に, マルウェアが出現してからシグニチャ型のアンチウイルスソフトが対応するまでには数日程度かかる[6]. このため, 本システムは, 既存のマルウェア対策に対して, 対応速度の点でも優位であると言える.

5 おわりに

本稿では, 著者らが研究開発を進めている「マルウェア対策ユーザサポートシステム」を用いて, CCC DATASet 2011 検体の検知・駆除を行った結果について述べた.

実験結果より, 本システムでは, マルウェアが作成するファイルパスが不変である場合は, ファイルを全て駆除することが可能であり, また, ファイルパスが不変でない場合であっても, ファイルが実行ファイルであるならば, 最終的に駆除することが可能であることを示した. また, 検知・駆除時間は最大でも 10 分程度であり, 従来のマルウェア対策と比較して, 対応速度が大幅に向上していることを示した.

今後は, システムのさらなる性能向上を図ると共に, 多数の一般ユーザを対象とした実証実験を通じて, 本システムの有用性を検証していく予定である.

謝辞

本研究は独立行政法人情報通信研究機構から委託を受けた「マルウェア対策ユーザサポートシステムの研究開発」の成果の一部を含みます. 本研究を進めるにあたって有益な助言と協力を頂いた関係者各位に深く感謝いたします.

参考文献

[1] 川口信隆, 他: マルウェア対策ユーザサポートシステムを用いた CCC DATASet 2010 の解析, マルウェア対策研究人材育成ワークショップ 2010 予稿集, 2010 年.

[2] D. Inoue, et al.: Automated Malware Analysis System and its Sandbox for Revealing Malware's Internal and External Activities," IEICE Trans. Information and Systems, Vol.E92-D, No.5, 2009.

[3] A.Lanzi, et al.: AccessMiner: Using System-Centric Models for Malware Protection", Proc. of 17th ACM Conference on Computer and Communications Security, 2010.

[4] 川口信隆, 他: マルウェア解析結果レポートに関する一検討, 2010 年度電子情報通信学会ソサイエティ大会予稿集, 2010 年.

[5] J. Oberheide, et al.: CloudAV: N-Version Antivirus in the Network Cloud, In Proc. of the 17th Usenix Security Symposium, July, 2008.