L-030

攻撃間の関係を用いた標的型攻撃確定手法の提案
A method to determine targeted attacks using the relation between attacks

片岡 えり† 松本 光弘† 白木 宏明†
Eri Kataoka Mitsuhiro Matsumoto Hiroaki Shiraki

1. 概要

標的型攻撃による被害が顕在化しているが、誤検知が多いという課題がある。そこで本稿では、標的型攻撃を確定する手法を提案する。本手法は、攻撃者が攻撃した端末のプロセス監視ログやネットワークアクセスログから、標的型攻撃の一連の攻撃間に関係があるかを抽出することで、標的型攻撃の有無を確定する。本手法を検証用に用意した 12 パターンの標的型攻撃に適用したところ、標的型攻撃を確定すると同時に、正常なログを攻撃と無関係だと判断できた。

2. 背景

2.1 標的型攻撃

標的型攻撃は、ここ数年被害が顕在化しているサイバー攻撃の一種であり、特定の組織内の機密情報の窃取を目的として行われる。標的型攻撃の例を表 1 に示す。このように、複数の攻撃を組み合わせて長期的かつ段階的に進行する特徴を持つ。こういった攻撃は攻撃対象の独自の脆弱性など、対象に特化した攻撃が行われるため、検知が困難である。

表 1 標的型攻撃例

#	攻撃フェーズ	攻撃手法	攻撃内容
1	調査	ソーシャルエンジニアリング	攻撃対象調査
2	侵入	マルウェア感染	メール添付ファイル開封
3	探索	スキャニング	セキュリティ脆弱性探索
4	遠隔操作	バックドア設置	侵入口を設置して通信経路確保
5	情報漏洩	―	機密情報の窃取

2.2 既存手法と課題

居城ら [1]は、標的型攻撃が段階的に進行することを利用して、たとえ未知のマルウェアであっても検知できる手法を提案している。この手法は攻撃の組合せを攻撃シナリオとして定義し、監視する通信の振る舞いと合致したものを攻撃として検知する。しかし、攻撃者が行う操作は正規のユーザも行う操作であり、正規操作がシナリオと合致した場合に攻撃として検知し、誤検知となる場合がある。

中里ら [2]は、プロセスの親子関係を示したプロセスツリーを生成し、予め生成したプロセスツリーと比較することで不審通信を検知する手法を提案している。この手法では、通常生成されないプロセスをいち早く検出し、攻撃を早期に検知できる一方、正常プロセスツリーの生成時に現れなかった出現頻度の低いプロセスを不審な挙動とみなして検知してしまう。

このように、誤検知の削減と早期検知の両立が課題となっている。

† 三菱電機(株) 情報技術総合研究所

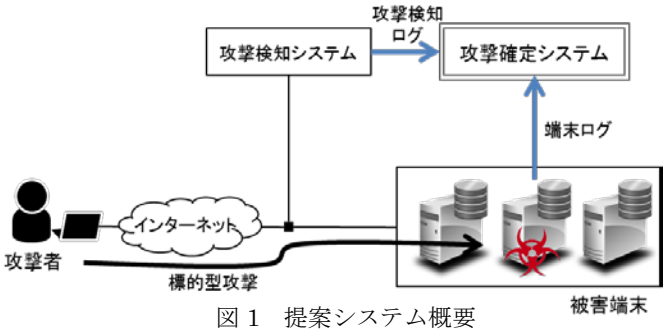

図 1 提案システム概要

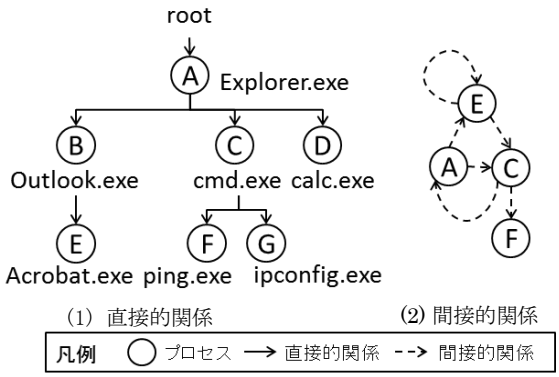

図 2 攻撃間の関係の構造例

3. 提案手法

本稿では、標的型攻撃における誤検知の削減と早期検知を目的として、攻撃間の関係に着目した攻撃確定手法を提案する。

3.1 概要

提案する手法を適用するシステムの概要を図 1 に示す。この手法は、攻撃シナリオを用いた攻撃検知手法 [1]の検知結果（攻撃検知ログ）を用いて、検知した攻撃を攻撃候補と位置付ける。そして、攻撃候補が一連の標的型攻撃かどうか確定することで誤検知を削減する手法である。確定には攻撃検知ログの他に、標的型攻撃の被害端末のログ（端末ログ）を用いる。攻撃確定システムには攻撃確定手法が組み込まれ、2 つのログから攻撃を確定する。

3.2 攻撃間の関係

まず、攻撃間の関係を(1)直接的関係と(2) 間接的関係として定義する。(1) 直接的関係は、2 つのプロセス間に親子関係（呼び出し元・呼び出し先の関係）、もしくは祖先・子孫の関係がある場合とし、(2) 間接的関係は 2 つのプロセス間にファイルアクセス、もしくはネットワークアクセスの関係がある場合とする。

攻撃間の関係の構造例を図 2 に示す。この例はメールの添付ファイルを開封すると同時に、添付ファイルに含まれ

Copyright © 2016 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.

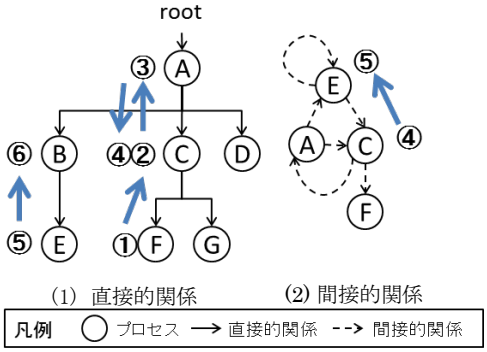

図 3　探索例

ていたマルウェアに感染し、攻撃者にネットワークを探索されている例である。(1) 直接的関係はプロセスの呼び出し元・呼び出し先の関係が一意に決まるため木構造になる。例えばメールソフトから PDF 閲覧ソフトを起動する関係（B→E）などがこれにあたる。一方(2) 間接的関係はファイルアクセスやネットワークアクセスなどの関係から、自分のプロセスを含む複数のプロセスからアクセスされる可能性がある。そのため、直接的関係と比べて複雑な構造になる。例えば PDF 閲覧ソフトのファイルシステムが自分のプロセスにアクセスする関係（E→E）などがこれにあたる。

3.3 関係探索

本稿では標的型攻撃の候補となる攻撃をプロセス単位で判断することとし、3.2 節で挙げた 2 種類の関係が攻撃間にあるかどうかを探索する。直接的関係ではプロセスの呼び出し関係を見ることができるが、他のマルウェアをダウンロードして攻撃するなどしてプロセスの呼び出し関係が切れた場合に関係を捉えることができず、一連の標的型攻撃として検知できない。そのため、関係するプロセスについて間接的関係も探索する必要がある。

プロセスの探索は、まず直接的関係を探索し、次に間接的関係を探索する。これらを発見されたプロセスについて再帰的に行う。直接的関係の探索はプロセスツリーの子から親の方向に探索する。これにより、探索するプロセスの関係を 1 つのパスに絞ることができ、探索回数を削減できる。また間接的関係については、端末内で発生した操作の発生時間に基づいて探索する。これにより探索するプロセスを絞り込み、関係のないプロセスの探索を削減できる。

3.4 探索例

図 2 の例において、3.3 節の手順でプロセス F の関係を探索した場合の探索例を図 3 に示す。まず、F のプロセスについて直接親（直接的関係の親）と間接親（間接的関係の親）の探索を行う。F の直接親は C であり、発見されたプロセスについて再帰的に探索を行うため、次に C の直接的及び間接的関係を調べる。C の直接親として A が発見され、同様に A の直接的及び間接的関係を調べる。A の直接親はないため、A の間接親について調べる。すると C が発見されるが、C は調査中のプロセスのため処理を終了する。これで A の探索は終了となり、C の間接親探索に戻る。同様に繰り返して F と関係するプロセスを洗い出すと、最終的に C、A、E、B の順に関係プロセスを発見できる。

表 2　検証した攻撃例

#	攻撃	攻撃内容
1	侵入	マルウェアの開封
2	探索	ユーザ情報の取得
3	遠隔操作	新たなマルウェアを被害端末にダウンロード
4	情報漏洩	被害端末内のファイル窃取

4. 評価

4.1 検証環境

仮想マシン上に攻撃端末と被害端末を用意し、12 パターンの標的型攻撃を実施して提案手法の検証を行った。これらの攻撃は検証用に作成したもので、脆弱性検証ツールである Metasploit Framework [3]を用いて複数の攻撃を組み合わせることで標的型攻撃を模したものである。攻撃を行っている間の被害端末のログを、Process Monitor [4]を用いて収集し、検証に用いた。

検証で実施した攻撃の一例を表 2 に示す。この例ではまずマルウェアが侵入し、被害端末で起動する。起動したマルウェアは端末内を探索し、新たなマルウェアを被害端末にダウンロードする。最後に、マルウェアが被害端末内の機密情報を窃取する。

4.2 結果

端末ログと攻撃検知ログを用いて検証を実施した。本検証では、攻撃プロセスと正常プロセスが混在したログを攻撃検知ログとして用いた。そして、攻撃検知ログから標的型攻撃を確定できるかどうか検証した。その結果、12 パターン全てにおいて攻撃プロセスを一連の標的型攻撃として確定し、同時に、正常なログを攻撃とは無関係だと判断できた。

5. まとめと今後の課題

標的型攻撃の誤検知削減および早期検知を目的として、攻撃候補間の関係から一連の攻撃を紐づけ、標的型攻撃として確定する技術を提案した。本稿では、提案手法を 12 パターンの標的型攻撃に適用し、攻撃のみを確定できた。これにより、誤検知の削減を実現できる見込みを得た。

今後の課題として、今回用いたログよりも詳細にグを収集し、関係の探索に活用することを検討している。これは、攻撃者の高度な攻撃、例えばなりすましやプロセスの書換えなどを捉えるためである。

参考文献

[1] 居城秀明, 河内清人 , 桜井鐘治, “攻撃シナリオを用いた多段攻撃検知手法の検討,” 情報処理学会第 76 回全国大会, 2014.

[2] 中里純二, 津田侑, 高木彌一郎, 衛藤将史, 井上大介 , 中尾康二, “ホスト型 IDS を用いた不審プロセスの特定,” 暗号と情報セキュリティシンポジウム（SCIS）, 2015.

[3] D. Kennedy, J. O'Gorman, D. Kearns , M. Aharoni, 実践 Metasploit ペネトレーションテストによる脆弱性評価, O'REILLY JAPAN, 2012.

[4] “Process Monitor,” [オンライン]. Available: https://technet.microsoft.com/ja-jp/sysinternals/processmonitor.aspx.

Copyright © 2016 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.