Activity Report 03

Project Theme 暮らしを支える安全・安心のインビジブル・セキュア・プラットフォーム

不正・有害な動作を行うマルウェアの正体を探　る動的解析システム

情報セキュリティを脅かすマルウェアの挙動を解析するシステムを開発しました。

いまや社会のあらゆるところに情報技術が浸透し、ネットワークが張り巡らされています。情報技術は非常に便利である反面、私たちの社会や生活を脅かす危険もはらんでいます。私たちのプロジェクトが目指すのは、こうした脅威を払拭し、安全・安心なネットワーク社会を構築することです。そのためにソフトウェアの開発から生成、実行まですべての段階でセキュリティを確立し、強固なプラットフォームを形成しようとしています。

個人情報の窃盗、組織や企業への攻撃やスパイ行為、さらには国家に対するサイバーテロまで、近年情報技術に関わる問題はますます増加し、かつ深刻なものになっています。こうした不正で有害な動作を行う悪意あるソフトウェアは、コンピュータウィルスやワーム、スパイウェア、トロイの木馬などさまざまに名づけられていますが、総称してマルウェアと呼ばれます。マルウェアの数は年を追うごとに増加しており、2011年の1年間だけで4億300万種を超える新種が出現したといわれています。こうした脅威を防ぐ有効なセキュリティ対策を講じるためには、まずマルウェアの挙動を熟知する必要があります。そこで私たちが開発したのが、マルウェアの挙動を解析するシステム“**Alkanet**[*1]”です。

解析時間を短縮し、アンチデバッグ機能を回避するVMMを用いた動的解析システムを開発しました。

Alkanetは、従来のマルウェア解析システムの課題を解決する画期的な特長を備えています。その一つは、短時間でマルウェアの挙動を把握できることです。1日に数千もの新種や亜種が出現する現状で、時間をかけて一つのマルウェアを解析していたのでは、出現スピードに追いつけません。より多くのマルウェアに対策を講じるためには解析の時間短縮が必須の課題です。そのための有効な手だてとして、実際にマルウェアを実行し、その動作を観測する動的解析によってマルウェアの挙動を把握する方法を採用しました。

二つ目は、マルウェアに動作解析ツールの存在を検知されないようにしたことです。最近のマルウェアの多くがアンチデバッグと呼ばれる機能を備えており、マルウェア自身が動的解析されていることを検知し、実行を停止したり、解析を妨害しようとします。そこで動的解析ツールを隠ぺいする、あるいはマルウェアのアンチデバッグ機能そのものを無効化するなど、マルウェアに検知されない方策が必要になります。私たちは、動作解析を妨げるようなマルウェアの機能を抑制するため、仮想計算機モニタ（VMM）の中に解析機構を構築し、マルウェア動作環境（マルウェアが動作するOS）と分離させる方法を考えました。VMMは、マルウェア動作環境よりも高い権限で動作するため、VMMからは、OSやその上で動作しているプロセスのすべてを透過的に監視することができますが、マルウェアからは解析機構を検出できないためアンチデバッグ機能の多くを回避できます。既存のマルウェア解析技術ではエミュレータを用いたものが多く、オーバーヘッドの大きさが課題でした。VMMを用いたものもありますが、それらがエミュレートするハードウェアの特徴からマルウェアに検出されやすくなってしまうという課題がありました。そこでAlkanetには、ホストOSを必要とせず、ハードウェア上で直接動作するハイパーバイザ型のVMM“BitVisor”を拡張機能として実装しました。これによってソフトウェアのみで実現されたエミュレータや既存のVMMより高速で動作し、マルウェアに存在を検出されるのも防ぐことが可能になりました。

マルウェアのシステムコールをトレースすることでプロセスを越えて拡散するマルウェアも追跡できます。

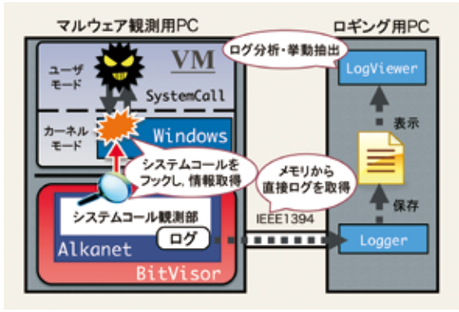
さらに三つ目のポイントは、マルウェアの挙動の意図をつかみやすい方法で観測し、より迅速に解析できるようにしたことです。そのために、マルウェアの挙動の追跡の単位を、プログラムの最小単位である機械語レベルではなく、抽象度の高いシステムコールレベルとしました。プログラムは通常、システムに影響を与えるような処理を実行する際には、その処理を提供するOS内のプログラムを呼び出す“システムコール”を使います。すなわち、これを追跡すればマルウェアの挙動を見逃すことはありません。近年は実行中に新たなプロセスを起動したり、他のプロセスに対してコードを書き込むなど一つのプロセスを越えて拡散するマルウェアが増加しています。マルウェアのシステムコールをトレースするこの方法なら、他のプロセスへ感染するマルウェアも追跡できます。

またシステムコールのトレースのログをさらに分析し、マルウェアの特徴的な挙動だけを抽出したレポートを出力するツールも合わせて構築しました。これによって、取得したシステムコールトレースのログから複雑なマルウェアや注目すべきマルウェアを選び出してコードを読み解く労力と時間を省略できます。

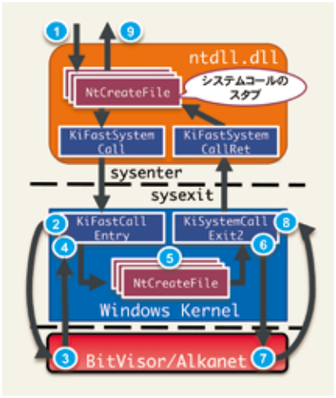
こうして構築したAlkanetがマルウェア解析に本当に有効かどうかを確認するため、すでに活動が記録されている実際のマルウェアを用いて解析を行いました。その結果、マルウェアのシステムコールを正確にトレースできたことに加えて、プロセスを越えて拡散したスレッドも区別し、追跡できることを確認しました。

マルウェアの解析ツールの開発に終わりはありません。いずれAlkanetの機能に抗体を持つ新たなマルウェアが出現することも十分想定されます。常にそうした新種のマルウェアの先手を打つ対策を講じ、機能をバージョンアップしていきつつ、今後はAlkanetを実際のマルウェア解析ツールとして実用化することを目指します。

［写真 左］
立命館大学情報理工学部 准教授
毛利 公一 プロジェクトリーダー
［写真 右］
立命館大学大学院情報理工学研究科 博士課程後期課程1回生
大月 勇人



Alkanetの全体構成



システムコールフックの流れ

（*1）**Alkanet** … 根を煎じたものに浄血や去痰などの薬効のある花の名前に由来。マルウェアに対する特効薬の原料になることを目指す。

●参考文献／**1** Alkanet: A Dynamic Malware Analyzer based on Virtual Machine Monitor. WCECS 2012, 1, 36-44（2012）. **2** マルウェアアナライザAlkanetによるマルウェア解析報告2012. CSS2012論文集, 2012, 3, 106-113（2012）. **3** マルウェア挙動解析のためのシステムコール実行結果取得法. CSS2011論文集, 2011, 3, 95-100（2011）.
●連絡先／立命館大学 びわこ・くさつキャンパス 毛利研究室　電話：077-561-5061　http://www.asl.cs.ritsumei.ac.jp/