様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ６ 月 １０ 日現在

機関番号：１２７０１
研究種目：若手研究(A)
研究期間：2012～2014
課題番号：２４６８０００６

研究課題名（和文）実効性の高い標的型攻撃対策に関する研究

研究課題名（英文）Study on Effective Countermeasures for Targeted Cyber Attacks

研究代表者
吉岡　克成（Yoshioka, Katsunari）

横浜国立大学・環境情報研究科（研究院）・准教授

研究者番号：６０４１５８４１

交付決定額（研究期間全体）：（直接経費）　　8,200,000円

研究成果の概要（和文）：本研究は、近年問題となっている特定組織や個人への標的型サイバー攻撃に対する有効な対策手法をテーマに実施した。この分野の研究が効果的に実施されていない理由として、多くの研究組織において標的型サイバー攻撃の実態把握ができていない現状に着目し、情報共有を活性化するために攻撃で用いられた不正プログラム(マルウェア検体)の共有のための文書型マルウェアの匿名化手法を提案した。また、標的型攻撃で用いられることの多いリアルタイム遠隔操作マルウェアの効率的な観測手法を提案し、観測結果にもとづき、これらのマルウェアの通信を検知する手法を提案、評価した。

研究成果の概要（英文）：This research focuses on Targeted Cyber Attacks and their countermeasures. Considering that information sharing on targeted attacks is the key for the studies of this field, we first proposed a method to anonymize document malware samples used for the attacks. Moreover, we proposed methods to monitor and detect remote and administration tool (RAT), which is often utilized for targeted attack.

研究分野：情報システム・セキュリティ、サイバーセキュリティ、マルウェア対策

キーワード：標的型攻撃対策　マルウェア検体共有促進　遠隔操作マルウェア観測　遠隔操作マルウェア検知

１．研究開始当初の背景

マルウェア対策は，従来，主にアンチウイルスソフトのベンダにより実施されてきたが，2000 年代中ごろからマルウェアの数と種類の増加が著しくなると，人手による解析と対策が困難となり，自動解析や対策導出の研究が世界的に行われるようになった．我が国でも情報処理学会とサイバークリーンセンター運営委員会(総務省・経済産業省)が 2008 年から現在まで毎年マルウェア対策研究人材育成ワークショップを主催し，多くの企業や大学の研究者が研究発表を行っていることからも分かるように，マルウェア対策の研究が活発に行われている．本研究の応募者は，2005 年から継続してマルウェア対策の研究を実施しており，特にマルウェアの活動の広域監視，マルウェア自動解析，自動対策導出，解析環境の脆弱性指摘に関して多くの検討を行ってきた．

一方，近年，企業や政府機関を狙った標的型攻撃の問題が指摘されており，実際に 2011 年には防衛産業企業において国家安全保障に関わる重大なインシデントが発生している．これらの標的型攻撃は，ワームやマスメール型の攻撃のようにインターネット上を広く拡散するわけではないため，攻撃に関する情報が少なく，対策を困難にしている．また，アンチウイルス等の既存の対策技術では検知が出来ないような，ステルス性の高いマルウェアが用いられるため，攻撃の存在自体が長期的に認識されない場合も多い．このような新たな特徴をもつ脅威に対して，有効な対策技術の研究開発が進んでおらず，早急な対策が求められている．

２．研究の目的

標的型攻撃の対策研究が滞っている大きな原因の 1 つは，対策を導出する基礎となる攻撃関連情報の不足である．攻撃関連情報が集まりにくい理由として，(Ⅰ)そもそも標的以外には攻撃が届かないため，広域ネットワーク監視等によって攻撃を把握できない (Ⅱ)ステルス性の高いマルウェアが用いられるため，標的となった組織は攻撃の事実を認識できない (Ⅲ)標的となった組織が攻撃を認識できた場合にも，当該組織に関わる情報とマルウェア本体とが一体となっている場合は，積極的な情報共有が行われにくい(例: 被害組織に関わる内容が記載された文書にマルウェアが埋め込まれている場合など)ことが挙げられる．(Ⅰ)情報の集約については，例えば警察庁では全国約 4,000 の事業者等とサイバーインテリジェンス情報共有ネットワークの構築を行っており，今後，情報収集の枠組みの整備が期待されるが，(Ⅱ)と(Ⅲ)については多くの技術的課題がある．

そこで，本研究では，これらの問題を解決するために以下の 2 つの課題(A)(B)に取り組む．

(A)ステルス性の高いマルウェアの中長期的観測による動的検知手法

標的型攻撃では，アンチウイルス等により検知されないことを，事前に攻撃者が確認した上でマルウェアを用いる場合が多く，個々のマルウェアの特徴(いわゆる静的シグネチャ)との比較に基づく検知の効果が低い．そこで本研究では，静的シグネチャに依存しない検知方法としてマルウェアの実行時の挙動(ビヘイビア)に基づく動的検知を対象に研究を行う．近年では，ビヘイビアベースの検知手法が多く提案されているが，これらはマルウェア実行直後の比較的短期間の動作に注目し検知を行うことから，故意に動作を遅延させることで検知を回避するマルウェアが出現している．我々は標的型攻撃の多くが機密情報搾取を目的とし，遠隔の攻撃者から制御されて機密情報の探索，収集，漏洩を行うことに注目し，中長期的な挙動の観測により，これらの検知を行う手法を検討し，具体的手法の提案，実装，評価を行う．

(B)標的型攻撃の情報共有を促進するための攻撃関連情報のサニタイズ技術

標的型攻撃では，事前に攻撃対象組織への正規のビジネス文書を盗み出し，この文面を用いて偽のビジネス文書を作成し，これに文書閲覧ソフトの脆弱性を突く攻撃コードを埋め込んだ上で，攻撃対象組織の然るべき相手に電子メールで送付する方法が典型的である．このような攻撃をなんらかの方法で検出した場合，攻撃コードやマルウェア本体が埋め込まれた偽造文書を解析する必要があるが，この文書の内容は攻撃対象の組織に関連が深いため，第三者である研究機関への提供が積極的に行われない場合がある．そこで，本研究では，偽造文書に埋め込まれた攻撃コードやマルウェアの動作については手を加えず，文書の文面だけを削除する方法，すなわち偽造文書のサニタイズ技術を検討し，具体的手法の提案，実装，評価を行う．

３．研究の方法

本研究では，平成 24 年度から平成 26 年度までの 3 年間で(A)ステルス性の高いマルウェアの中長期的観測による動的検知手法(B)標的型攻撃の情報共有を促進するための，マルウェア検体のサニタイズ技術，という 2 つの研究課題に取り組む．

まず，2 つの課題に共通する項目として攻撃情報・検体・攻撃ツールの収集を研究実施期間中，継続的に実施する．取得した検体および攻撃ツールは，提案手法の評価実験に用いる．また，安全に研究を行う基盤となる実験環境を 24 年度中に構築し，25 年度以降は

必要に応じて増強と機能の拡張を行う．課題(A)については 24 年度中に標的型マルウェアの中長期的挙動の観測を行うこととし，その観測結果を基に 25 年度において検知手法を提案し，26 年度に評価実験・手法の改良を行う．課題(B)については，24 年度中に具体的な手法の提案を行うと共に，25 年度以降は提案手法の評価実験，提案手法に対する新たな攻撃の検討，手法改良に取り組む．

４．研究成果

(A)ステルス性の高いマルウェアの中長期的観測による動的検知手法

標的型攻撃に用いられるマルウェアとして特に RAT(Remote Administration Tool)とよばれるリアルタイム遠隔操作型マルウェアに着目し、この検知を目標とした．研究の第一段階として RAT を用いた攻撃を効率的に観測する手法を提案した．具体的には、攻撃者が遠隔操作に用いる GUI の画面を観測時に再現する画期的な手法を提案し、情報処理学会コンピュータセキュリティシンポジウム 2013 学生論文賞、マルウェア対策研究人材育成ワークショップ(MWS)2013 学生論文賞を受賞し、情報処理学会コンピュータセキュリティ研究会推薦論文となった．また、国際会議 IWSEC2014 (International Workshop on Security)にて当該技術に関する招待講演を行った．

また、標的型攻撃の主な目的である重要情報の収集と漏洩という目的に着目し、ダミーの情報を保護対象システム内に事前に配置しておき、それらの情報へのアクセスや悪用を検知することで事後的に不正侵入を検知する手法を提案した．実際の情報漏洩マルウェアに対してこれを適用し、情報漏えい先や漏洩した情報を悪用する様子を観測すると共に、これらの活動を検知することで感染の事実を把握できることを示した．

さらに、企業などの保護対象システムにおいて想定される、保護対象ホスト群の状態の類似性に着目し、ホストの状態が他と逸脱していることを検知することで不正侵入を検知する手法を提案した．実マルウェア検体を用いて様々な侵入経路を想定した検知実験を行い，高い精度でこれらのマルウェアの検知が行えることを示した．

また、標的型攻撃の多くがビジネスメールなどに似せたメール添付マルウェアにより行われることに注目し、これらのマルウェアの特徴であるビジネス文書の表示に着目することでこれを検知する手法を提案した．実マルウェア検体を用いて検知実験を行い、高い精度で検知が実現できることと，正規プログラムの誤検知がないことを示した．

(B)標的型攻撃の情報共有を促進するための，マルウェア検体のサニタイズ技術

標的型攻撃の情報共有を促進するため、文書型マルウェアから標的に関する情報を削除・墨塗りする匿名化手法を提案した．実際に攻撃で使用されたマルウェアにこれを適用し、限定的ではあるものの、文書の墨塗りが可能であることを示した．

(C)上記以外の成果

上記に加えて、標的型攻撃における新たな侵入経路・情報収集の対象となる可能のあるスマートフォンに着目し、そのセキュリティの現状を調査した．具体的には市販の Android 向けアンチウイルスソフトの実力を評価するため、実マルウェア検体を用いてその検知率を評価した．特に実マルウェアに簡易な変更を加えた際に、多くのアンチウイルス製品の検知率が著しく落ちることを発見した．

標的型攻撃の目標の一つとなる制御システムのセキュリティに関する基礎検討を行った．具体的には、市販のネットワーク機器を用いた静的パケットフィルタリングの効果を各種の想定される攻撃に関して定性的に評価した．

これらの研究の基本データとして共同研究先から提供された標的型攻撃マルウェア検体を４０体以上詳細解析し、その特徴を調査し、検知技術の提案の基盤とした．また解析を行うための環境を整備した．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　0 件）

〔学会発表〕（計　9 件）

[1] 髙橋佑典，吉川亮太，吉岡克成，松本勉，″ダミー文書表示に着目した標的型マルウェア検知手法,″ 電子情報通信学会 ICSS 研究会，2015.

[2] Yusuke Takahashi, Masaaki Kobayashi, Yuehting Chen, Kazuki Yonemochi, Katsunari Yoshioka, and Tsutomu Matsumoto, “Observing RAT Server’s Behavior through Its Client GUI, IWSEC invited talk, 2014.

[3] 小林大朗，鉄穎，武部達明，鈴木和也，吉岡克成，松本勉，″生産制御システムにおけるセキュリティ強化のためのホワイトリストベースパケットフィルタリング,″ 情報処理学会コンピュータセキュリティシンポ

ジウム 2014, 2014.

[4] 吉川亮太, 神薗雅紀, 吉岡克成, 松本勉, ″保護対象ホスト群の状態の類似性に着目した悪性プロセスの検知手法の提案,″ 情報処理学会コンピュータセキュリティシンポジウム 2014, 2014.

[5] 高橋佑典, 小林大朗, 陳悦庭, 小山大良, 吉岡克成, 松本勉, ″RAT サーバの動作を遠隔操作者と同じ操作画面で観測する方法 その2,″ 情報処理学会コンピュータセキュリティシンポジウム 2014, 2014.

[6] 米持一樹, 田辺瑠偉, 吉岡克成, 松本勉, ″ダミーの認証情報を用いて不正侵入を事後検知する方法,″ 電子情報通信学会暗号と情報セキュリティシンポジウム 2013, CD-ROM 論文集, セッション 4C2-5, 2013.

[7] 齊藤真吾, 吉岡克成, 神薗雅紀, 星澤裕二, 松本勉, ″標的型攻撃情報共有のための文書型マルウェアの墨塗り手法,″ 情報処理学会コンピュータセキュリティシンポジウム(CSS2013)・マルウェア対策研究人材育成ワークショップ(MWS2013).

[8] 高橋佑典, 小林大朗, 陳悦庭, 米持一樹, 吉岡克成, 松本勉, ″RAT サーバの動作を遠隔操作者と同じ操作画面で観測する方法″, 情報処理学会コンピュータセキュリティシンポジウム(CSS2013)・マルウェア対策研究人材育成ワークショップ(MWS2013).(CSS2013 学生論文賞、MWS2013 学生論文賞、情報処理学会コンピュータセキュリティ研究会推薦論文)

[9] 庄田祐樹, 金井文宏, 森博志, 吉岡克成, 松本勉, ″Android 用アンチウイルスソフトは簡易な変更が施された既知の不正アプリを検知できるか？,″ 電子情報通信学会暗号と情報セキュリティシンポジウム 2013, CD-ROM 論文集, セッション 4C1-2, 2013.

〔図書〕（計　0 件）

〔産業財産権〕
○出願状況（計　0 件）

○取得状況（計　0 件）

〔その他〕
ホームページ等

攻撃者による RAT 遠隔操作をリアルタイム監視する手法について
http://ipsr.ynu.ac.jp/ratmon/index.html

６．研究組織
(1)研究代表者
吉岡　克成（YOSHIOKA Katsunari）
横浜国立大学・大学院環境情報研究院・准教授
研究者番号：６０４１５８４１

(2)研究分担者

なし

(3)連携研究者

なし