平成２４年度総合セキュリティ対策会議

「サイバー犯罪捜査の課題と対策」部会（第２回）

平成 24 年 12 月４日

発言要旨

１．開会

２．不正プログラム解析センターについて

【事務局から、不正プログラム解析センターについて説明】

３．日本及び海外におけるコンピュータ・ウイルスの現状及び対策について

【委員３名から、日本及び海外におけるコンピュータ・ウイルスの現状及び対策について発表】

○発表者１：今回の発表の重要なキーワードは「スレットインテリジェンス」になります。スレットインテリジェンスについての統一された定義はないと認識しておりますが、本発表中は「セキュリティ脅威を完全に理解するために必要な全ての情報及びそれによって生み出された知見」ということで定義をしています。そして、良質なスレットインテリジェンスはセキュリティ脅威に対抗するための判断、行動の助けになると考えています。

スレットインテリジェンスが、どのようにして作り出されているのか、主に３つのものがあります。

まず、アンチウイルスソフト等の製品がいわばセンサーになり、そこからさまざまな情報を集めるものです。また、これ以外にも、顧客のサポートの中で発生するさまざまなインシデントへの対応で得られた知見というものも、スレットインテリジェンスになります。さらに、全体の攻撃の傾向や、あるいは攻撃者に焦点を絞って、それぞれどのような攻撃者のグループがあるのか、またそれぞれがどのような特徴を持っているのかといった観点での調査分析も行います。

こういったものが全て総合されて、スレットインテリジェンスと呼んでいる脅威についての情報や知見というものが生まれることになります。

ここで、スレットリサーチとマルウェア解析という言葉についても、簡単に整理して

おきます。マルウェア解析は、基本的にはマルウェアの動作に関する事実情報を調べることと言えるかと思います。マルウェア解析は、脅威がマルウェア自身であった時代においては非常に重要であったわけですが、最近の脅威は標的型攻撃に代表されますとおり、マルウェアというのはあくまで手段として用いられているにすぎない状況ですので、マルウェアだけを見ていても脅威の全貌というのは見ることができない状況にあります。

そこで、脅威の全貌を知るために行っている取組がスレットリサーチというものになります。マルウェア解析は非常に重要なものですが、それを基礎としてさまざまなつながりですとか、あるいはより高い視点から攻撃全体の状況を俯瞰したり、また過去からの経緯を踏まえた流れ等を考えたりして、攻撃者の目的ですとか手法の傾向の分析を行うことが今、必要になっています。これがスレットリサーチになります。

実際にスレットインテリジェンスを使って、顧客の環境をどのように守っているのかというと、組織のネットワークの出入口に対してセンサーを設置して、そこで通信の状況を監視し、不審な通信、あるいは不正な通信を分析しています。センサーによって集められた情報を分析担当者が分析して、顧客に対して今、注意するべきものが何かといったことをレポートにまとめて報告するといった活動を行っています。

最後に、スレットインテリジェンスとの官民連携として、１つキーワードになるのが「情報連携」であると考えています。官民がそれぞれの立場で得ている情報をうまく相関して、有益な情報にまとめることが非常にキーになってくると考えております。

○発表者２：グローバルレベルの約数百人の有識者に今後のセキュリティに関する予測について、見解を相互に精査し、議論を交わした上で、当社は 2013 年のセキュリティに関する予測を発表しました。その中では今後の予測として、ソーシャルネットワークの収益化に伴う脅威の増大、サイバー上の対立図式の一般化、モバイルを狙ったアドウェアの横行、モバイルとクラウドへの移行等を挙げています。モバイルとクラウドへの移行については、ユーザーの行くところに攻撃者ありということで、今年、アンドロイドのマルウェアが急増したのも、それを裏付けていると思います。

加えて、最後に新たな脅威としてのランサムウェアです。ランサムウェアとは、何らかの方法でコンピューターの機能を無効にして、正常な状態への復旧、復元の引き換えに金銭を不正に要求する悪質なソフトウェアです。2009 年に登場しまして、当初単純に画面をロックしてコンピューターへのアクセス復元のために金銭を要求するだけというものが多かったのですが、最近、非常に巧妙化しておりまして、一昨年ぐらいからはオ

ンライン送金の仕組みを巧みに使って、実際にお金をとってしまうものが現れてきております。今後の予測ということで説明させていただきました。

次に、現状の考察です。悪質な攻撃、マルウェアメールとウェブによる脅威というのは全体的には減少傾向にあるものの、まだまだ主流な経路になっています。今回の一連の遠隔操作ウイルス事件もそういった傾向があったかと見ています。

マルウェアメールとウェブによる脅威がまだまだ多いということを共有した上で、今後の対策を考察させていただきます。通常、明らかに不正なプログラム、既知の悪質なファイルというのは、それを検知するためのいわゆる定義ファイルと言われるもので対応するのが今まで一般的でした（ブラックリスト方式）。一方、信頼できるプログラムファイルというのは、多くのユーザーに利用され、使用されているので、いわゆるホワイトリストみたいな形で安全と見ることもできる。しかし、ほとんど誰も使用したことがなくて、ファイルの情報元も不明だったり、良いファイルなのか悪いファイルなのか判断が難しかったりして、ブラックリストでもホワイトリストでも対応できないプログラムのリスクといった問題があります。

それを逆手にとる形で、経験則に基づく判断で、普及度が少なくて利用者が少ないファイルで、ファイルの情報元が不明なものに関しては、評価、信頼が低いと判断して、リスクを伴うファイルと検知するような技術、これをレピュテーションと呼んでいます。当社ではこれらの一連の技術を製品に実装しています。

また、振る舞い検知と呼ばれるものがあります。これはインストールされるプログラムがマルウェアによく見られる特性を示した場合に、ユーザーに警告を出すようなものです。当社はこの技術も実装しております。

この２つの技術が定義ファイルの限界を補う技術ということです。

今回の一連の遠隔操作ウイルス事案のような場合、定義ファイルを作成するまでに非常に時間がかかる結果、侵入されたことを気づかないまま使っていることがありますので、こういった技術を使って早期に警告を出すという仕組みで、安全なインターネット環境を実現していきたいと思っています。

なお、今回の遠隔操作ウイルスについては、定義ファイルでは検知できなかったのですが、レピュテーションでも、振る舞い検知でも警告を出したということが事件後の検証で判明しています。

最後に、今後の対応に関しては、基本行動の大切さということと、また、アンチウイ

ルスベンダーとしては、新しい技術をどんどん使ってもらうようにということで、継続した普及活動をどんどん仕掛けていきたいと思っています。顧客には、疑わしいリンクや添付ファイル、ウェブサイトの不審なリンク等はクリックしないということを注意喚起させていただくとともに、ＯＳやインストールされている各ソフトウェア、これは常に最新の状態に保つ。そして、不明なソースからソフトウェアをダウンロードする際には、十分注意するという基本行動の大切さを伝える。そこに、振る舞い検知だったりレピュテーション等の技術を組み合わせたりという対応が、マルウェア感染等を防ぐ確実な一歩になるかと考えております。

○発表者３：本年度、当社はサイバー防衛に関する報告書を出しました。

報告書で挙げたサイバー空間の非常に大きな問題としては、やはりサイバー犯罪に関しては、儲かるだけではなく、リスクが低く、匿名で実行することが可能だということです。また、犯罪者は動きが迅速で資金も豊富にあります。情報共有に関しても法的な制限がなく自由にできるので、非常に動きが速い。さらに、攻撃対象はほぼ無制限だということで、非常に頭の痛い問題であります。

報告書では、リスク／迅速性成熟度モデルというものをベースに各国のサイバー対策の取組を紹介しています。このモデルでは、リスク管理、セキュリティの耐性がどれだけ強いのかということと、迅速性、犯罪への対応スピードが正比例すると整理されています。リスク／迅速性のレベルとしては、事故が発生した後に対応と対策を行うＥ「事後対応」から、断片的にツールが導入されているＤ「ツールベース」、そして、ツールが面として導入され全体状況を迅速に把握できるＣ「統合ピクチャ」、迅速な対応が可能なＢ「動的な防御」、各種攻撃を受けている場合でも、通常のシステム運用が可能なＡ「高い耐性」まであります。

このモデルでは、「状況認識の向上」という言葉がキーワードになります。各国の犯罪捜査機関であれ、防衛機関であれ、このキーワードが非常に大事になってきます。状況認識がしっかりできていれば、高い予測に基づいて迅速に捜査活動ができるということです。

サイバー空間の中での状況認識の向上においては、例えば送信元の情報、どこから攻撃が来ているのか、敵の規模、個人でやっているのか、複数でやっているのか、それともプロの集団が行っているのか、攻撃の意図は何か、攻撃の種類は何かということを、迅速に把握することが重要です。また、既に侵入されているのかどうか、不審な動きが

あるのかないのか、自社のシステムの中で弱点や脆弱な部分はあるのか、またセキュリティ意識の低い人間がいるのかいないのか、迅速な対処措置ができるのか、といった点を把握することも重要です。

ここで、状況認識の向上を可能にするのがレピュテーションになります。情報を一極で統合し、時系列で全部相関分析ができるということまでしないと、なかなかサイバー空間における状況認識は向上しません。例えば、このＩＰアドレスはこのＩＰアドレスといつ連携したのか、このＩＰアドレスからどういったファイルをもらったのか、どういったウイルスに感染しているのか、もらったのか、そのウイルスはどこへ拡散していったのかということを、全部データベースの中で時系列で押さえています。そこまでしないとなかなかサイバー空間の状況認識は分かりません。

当社は、そういった情報をリアルタイム・自動的に製品に対して配信をして、検知したり防御したりする仕組みを提供しています。

最後に、各国の政府の、特に捜査機関とどのように協力してサイバー犯罪と戦っていくのかということなのですが、大きく分けて３点あります。

１番目に、Legal Frameworks & Law Enforcement。法執行機関に対する協力として、情報収集して得られた知見を取りまとめ、各国の犯罪捜査機関や司法当局に対してレポートを提供しています。また、トレーニング、勉強会、セミナーを開催することも可能です。

２番目に、Education & Awareness。やはり意識を高める必要があることから、教育の提供等もしています。

最後に、民間企業として一番大事なのが、Technology & Innovation。過去何十年、アンチウイルス、ブラックリストという形で、製品を出してきましたが、なかなか検知できないということで、大きな問題点になっています。そこで、我々の責任として新しい技術に基づく製品をもっと簡単に、もっと一般の市民が使いやすい形で提供していかなければ､サイバー犯罪と立ち向かっていくことは難しいのではないかと考えております。

４．質疑応答

○　都道府県警察に不正プログラムの情報提供がどのようになされるのか、また、それがうまく機能しているのかどうかについて教えていただけたらと思います。

○事務局：都道府県警察に対しては、改正刑法に基づいて相談等で入ってきていると聞い

ています。また、これまでも標的型メール攻撃については情報が入ってきているところです。これらの枠組みは機能していると考えています。

○　発表された３名の方に共通の質問ですが、ボットネットについて、今動いているボットネットはどういったものがあって、今誰がその制御を持って、どういうコマンド、どういう目的で行使しているのかというプロファイリングを行うのが本来のインテリジェンスだと思いますが、標的型攻撃者については、そのようなプロファイリング等のインテリジェンスにどのぐらい踏み込んでいるのか、教えていただければと思います。

○発表者１：標的型攻撃の攻撃者についての分析がどこまで進んでいるのかということですが、当社は世界の研究機関と共同でリサーチ等を行っております。

　そこで、大体どの程度の数の不正プログラム、バックドアが利用されているか、そこからどの程度の攻撃者グループが存在しているのか、また、そこで攻撃者グループが実際に組織ネットワークに侵入をして行うときに、どのような手法で情報を探して、そして持っていくのかといったことについて、ある程度分かっていることはあります。このような調査活動で、公にできることについてはリサーチペーパーという形で公開しております。

○発表者２：当社も、全世界の主要な研究機関と共同で、リサーチを実施しています。ホワイトペーパーや、研究機関のアウトプットという形で、広く各種の情報のアナウンス等を行っています。

○発表者３：大まかなところは脅威レポートということで、四半期ごとに出しています。非常に顕著な動きとしては、経済の状況とサイバー犯罪が比例関係にあるということです。優秀な人材がなかなか職を得られない場合、サイバー犯罪の数字も上がっていくということがあり、そういった全体的な社会的な動きも大事だと思っています。

○　予防的な情報を確認・収集することが将来的な防犯、あるいは犯罪手法の解明ということにつながっていくと思います。そこで質問ですが、ＩＰがどこからどこへ流れているかなど、いろんな情報を集められていると思いますが、個人の場合であればプライバシー、企業であれば、企業の利益、それらの保護についてはどのように考えれば良いでしょうか。

○発表者３：サイバー犯罪への対応については、発表でも申し上げたとおり状況認識の向上が必要ですが、絶対にプライバシーとの関わりが問題となります。特にヨーロッパ諸国では、プライバシーは非常に重要です。例えば、ＩＰアドレス自体もこれは個人情報

じゃないかと考えている向きもあります。

ただ、当社の運用としては、プライバシーに抵触しないような形でやっています。非常に気をつけなければならない問題ですが、同時に、情報を収集して状況認識を向上させないと、捜査が行き詰まってしまうという問題もあるかと思います。

○　発表にあった、Legal Frameworks でどういうことを想定されているのかということと、Law Enforcement との関係について御説明いただければと思います。

○発表者３：サイバー犯罪の大きな問題は、現在の刑法ではなかなか対処できなくなりつつあるということです。攻撃者のほうが新しい技術を使ってくる。司法当局が、最新の脅威の情報であるとか、技術的な話をなかなか理解できない。

ですので、定期的に全体像、どういう組織的な動きがあるのかということを司法当局に説明しています。海外で起こったサイバー攻撃やサイバー犯罪は必ず日本でも起こり得ます。世界各国の状況を知って予測しておかないと、起こってから対策をしようとすると遅くなってしまうということです。

Ｔｏｒについても同様です。やはり情報収集をしないと、サイバー犯罪に対してなかなか適切に対応できないということが大きな問題点だと思います。

○　リスク／迅速性成熟度モデルにおいて、日本の企業やユーザーはどのレベルにあるのか。踏み台になるような可能性のある一般の企業やユーザーを見たときに、一体どういうレベルにあると認識しておけばいいのかということに関して、何かコメントがあればお願いします。

○発表者３：日本の企業のレベルは様々ですが、概ねＤ「ツールベース」のレベルだと思います。セキュリティの意識はあって、いろんなセキュリティ製品はあるけれども、それが点として存在していて面として防御できない。要は、状況認識ができていない。点在しているセキュリティツール、センサーを統合する必要があるかと思います。