アンラボ・セキュリティレター

Press Ahn

2018.11　Vol.59

ラテラルムーブメント、正常と悪性の境界を越えて対応せよ

脅威の内部移動と対応について

ラテラルムーブメント、正常と悪性の境界を越えて対応せよ

企業を標的に持続的に攻撃を試みては内部インフラに入り込み重要な情報を奪取する知能型脅威は、知られていないだけで今この瞬間にもあちこちで発生している。知能型脅威の攻撃は少なくとも数ヶ月から数年かけて執拗に行われ、特に内部ネットワークを通じて展開されるため、最初に侵入したシステムと最終的に被害が発生したシステムが全く異なる場合が多い。よってインシデントが発生した際に正確な被害を把握し、再発を防ぐため「ラテラルムーブメント(Lateral movement、内部ネットワーク移動)」を逆追跡できる対策が必要だ。ここでは最近注目されているラテラルムーブメントの概念と攻撃方法、対策について紹介する。

ラテラルムーブメント(Lateral Movement)は、直訳すると「横方向移動」だが「内部移動」、「内部拡散」などと解釈できる。ラテラルムーブメントを横方向移動に制限すると「縦方向移動(Vertical Movement)」の概念も存在し得る。同一線上での移動、例えばクライアント対クライアント(Client to Client)、サーバ対サーバ(Server to Server)などは横方向移動といえるが、クライアントからサーバへ(Client to Server)、サーバからクライアントへ(Sever to Client)の移動は縦方向移動と見ることができる。ここでは更に汎用的な意味として「内部ネットワーク移動」の概念で捉えて説明した。

シンプルに定義すると、ラテラルムーブメントは知能型脅威(Advanced Persistent Threat、以下「APT」)の攻撃過程の中で、攻撃者が組織内の最初のシステムハッキングに成功した後、内部ネットワークで使用されるアカウント情報を獲得して内部ネットワークシステムに移動する方法を指す。攻撃者はなぜラテラルムーブメントをするのか。その理由は、皮肉にも企業のセキュリティに対する認識と対応レベルが高くなるにつれて境界セキュリティが強化されたためである。そのため攻撃者が特定の組織を標的にするとしても、特定のシステムを直接一気に突き通す可能性が段々減ってきている。それ故に一般ユーザーが利用するクライアントシステムへと内部進入ベクター(vector)を変更した。ユーザーシステムを先にハッキングした後で攻撃者が望むデータが保存されている内部の別のシステムを探り、内部から内部に移動することが必要となった。
数年前から APT 攻撃のリスクが続き、攻撃規模はどんどん大きくなっている。一部の攻撃グループは国の支援を受けているのが分かった。明確にその数を把握することはできないが、これまで公開された情報だけまとめても 200以上の攻撃グループが活動している。攻撃者の目的は機密資料、個人情報、ゲームマネー、仮想通貨などの情報や資産を略奪するだけでなく、インシデントの公開、サービス拒否(DoS)、ランサムウェアなどの脅迫によって金銭的な利得を得ようとするのがほとんどである。

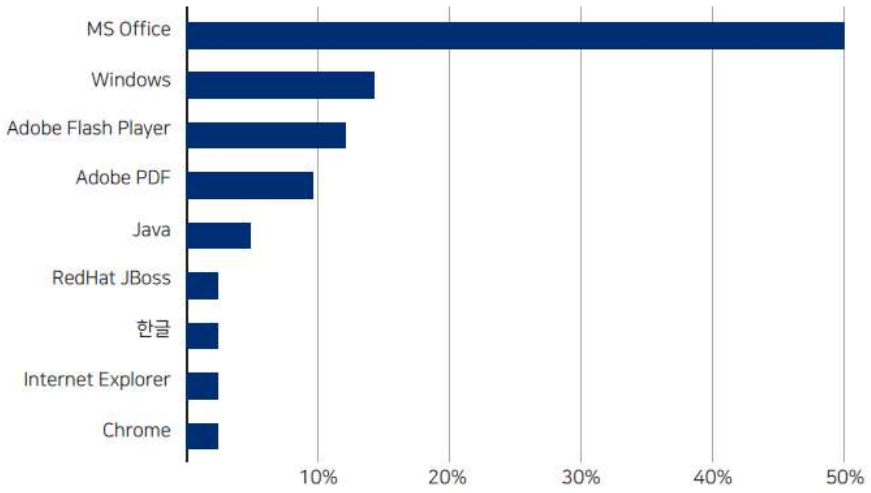
外部から内部へ侵入する

APT 攻撃の段階を説明するモデルは様々で、用語やステップに一部差はあるが大きな違いはない。APT 攻撃の段階は、外部から内部へ移動することと内部から内部に移動することで大きく 2つに分けることができる。

まずは外部から内部への移動を探ってみよう。攻撃者は特定の組織を標的にして該当の組織に対する様々な情報を収集する。標的組織のインフラを把握することも含めて標的組織を攻撃するためのツールを準備する。この際、標的組織で使用するセキュリティ製品に検知されないために事前にアンチウイルス(Anti-Virus)検知テストをする場合もある。

外部から内部へのアクセスが強固に保護されている環境で、攻撃者が組織に侵入するために選択できるオプションは少ない。中でもこれまで侵入成功率が高く、標的型攻撃が可能な攻撃方法はスピアフィッシング(Spear Phishing)と水飲み場(Watering Hole)攻撃だった。簡単に説明すると、エクスプロイト(Exploit)コードがメールの添付ファイルに含まれていれば「スピアフィッシング」で、ウェブに埋め込まれていてリンクを伝えたり被害者がよく訪問するウェブサイトを変ざんしたならば「水飲み場攻撃」だ。

実際はこれら 2つの方法が混用される場合もあり、主に利用されるソフトウェアは Microsoft Office、Windows、Adobe Flash Player、Adobe Acrobat Reader などだ。これらの方法は外部から内部を攻撃するもので、クライアント端末を狙った攻撃だった。

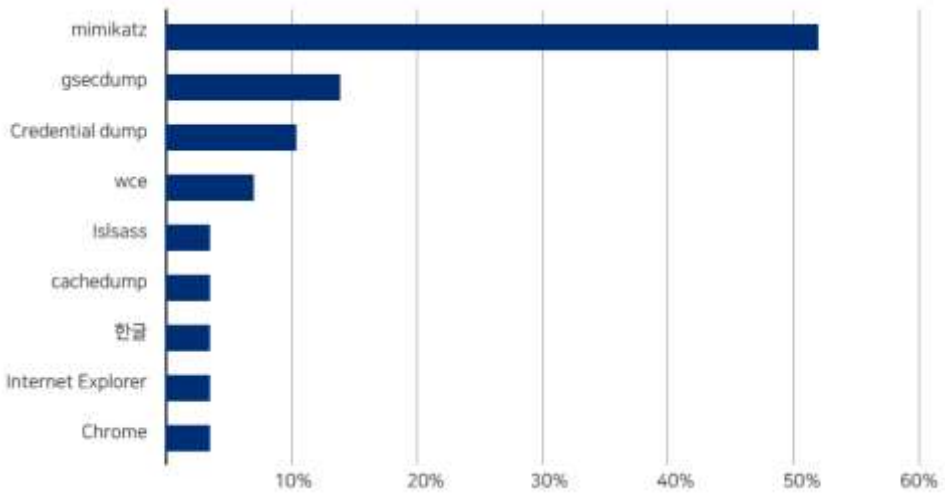


[図 1] APT 攻撃に使われた主なソフトウェア

攻撃者はユーザー PC を攻撃するため、当然ながらユーザー PC でたくさん使われるソフトウェアを狙う。この際、ソフトウェアの脆弱を利用するエクスプロイトコードが動作すれば、外部にある攻撃者の C&C(Command & Control)サーバとアクセスすることが可能となり、攻撃者は標的組織のネットワークに存在するクライアント端末を直接コントロールできるようになる。外部から内部へ移動したのである。

内部から内部に移動する

攻撃者が内部ネットワークに存在するシステムの制御権を得られたら目的を達成するまでできるだけ密かに動き、その期間はかなり長期にわたる可能性もある。ただし内部ネットワークに侵入した以上、内部ネットワークを通じて別のシステムにアクセスするのは比較的容易だ。ほとんどのセキュリティ製品は、外部から内部へ進入する場所に集中しているためだ。内部ネットワークで移動する際に、最近攻撃者が主に使う方法はシステムにアクセスするために認証情報(Credential)を盗み、それを利用して内部ネットワークの他のシステムに移動することである。盗んだ認証情報がハッシュ(Hash)タイプならば「Pass-the-Hash」攻撃と呼ぶ場合もある。認証情報を盗むツールは様々だが、その中で Mimikatz と呼ばれるツールが最も多く使われる。Mimikatzは SAM レジストリやメモリから Windowsアカウント情報をダンプ(Dump)できる。



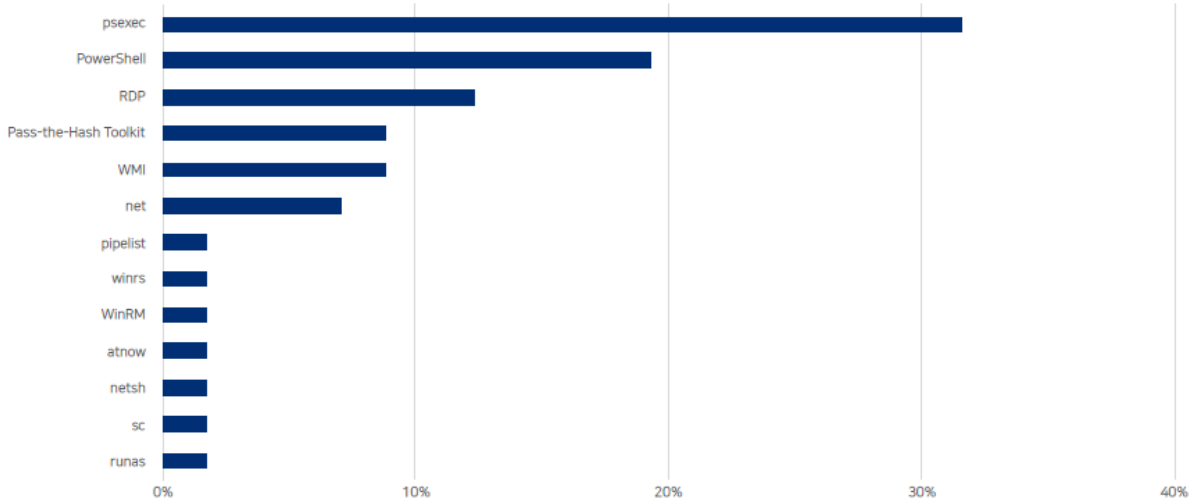
[図 2] APT 攻撃に利用される認証情報獲得ツール

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 356353 (00000000:00057001)
Session           : Interactive from 1
User Name         : user7321
Domain            : AFIRSTTEST
Logon Server      : DC01
Logon Time        : 2018-08-28 오후 5:32:09
SID               : S-1-5-21-2380026804-1514439288-2875446858-1109
        msv :
         [00000003] Primary
         * Username : user7321
         * Domain   : AFIRSTTEST
         * LM       : 49d27c643b07b7b83263b7f408b92a64
         * NTLM     : 5d5c76de95767608243c0dd149eb89fd
         * SHA1     : 907c12104f83ad0cbabc7b2eae1766e5558d52d5
        tspkg :
         * Username : user7321
         * Domain   : AFIRSTTEST
         * Password : u7321P@ssw0rd!
```

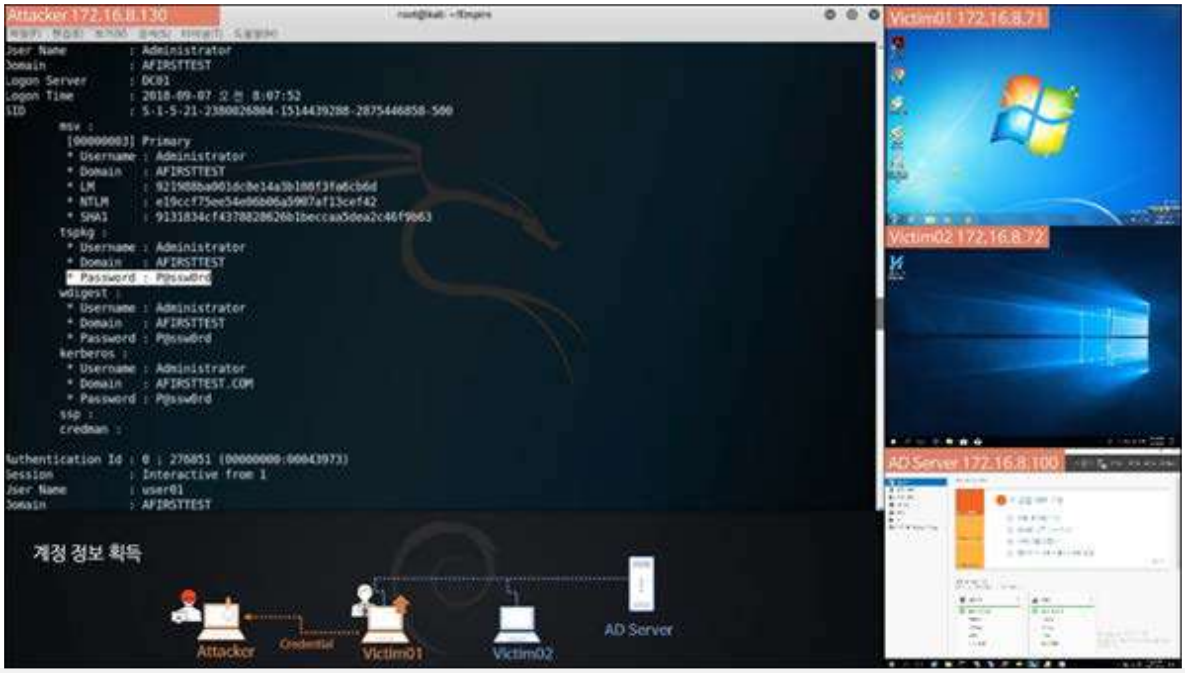
[図 3] Mimikatz(Mimikatz)実行画面

攻撃者が平文タイプ、又はハッシュタイプの認証情報を獲得した以降は、それを利用して該当のユーザーに装って別のシステムにアクセスできる。ここで最も頻繁に使われるツールは PsExec、PowerShell、RDP などがある。



[図 4] APT 攻撃に利用されるラテラルムーブメントツール

最近は、特に PowerShell を利用した攻撃が多発している。Windows システムには PowerShell が基本的にインストールされており、強力なシステム制御機能を提供するため管理者だけでなく攻撃者にも非常に注目されている。数年前から PowerShell を利用して内部侵害後のプロセスを制御できるフレームワークが多く公開されてきた。公開されたフレームワークには Powersploit、Nishang、Empire、Pupyなどがある。



[図 5] Empireを活用した侵害シミュレーション

インシデントを認知する

このような APT タイプの侵害が発生した場合、認知する方法はいくつかある。まずは組織内のシステムで異常なファイルや DB 変更、そして不正アクセスなどが発見されたり、更に深刻になるとシステムやネットワーク障害が発生するケースもある。もちろんセキュリティ製品やサービスによって脅威が検知される場合もある。その反面、外部から侵害を認知する場合もある。外部からインシデントの報告が入ったり、ネット上で出回る会社の機密資料を確認することもある。そしてランサムウェア攻撃のように攻撃者から直接脅かされる場合もある。

組織はこのような内外の状況から侵害を認知するが、残念ながらほとんどの組織は侵害を認知するのに平均 170日以上かかるという。これはグローバル平均値であり、韓国を含むアジア圏の場合は更に長時間かかるといわれている。アンラボのフォレンジック専門担当組織(A-FIRST)の分析事例には、大企業で 2年経っても認知できていない場合もあった。それぐらい時間が経過すると既に攻撃者は目的を全て達成したと考えられる。

インシデントの認知が遅れるのはいくつかの理由がある。一つ目に、組織内で侵害を認知するための活動(脅威ハンティング、Threat Hunting)をしないことだ。二つ目は、マルウェアを検知した場合に原因を把握せずにアンチウイルスによる治療やシステムフォーマットなどの単純な対応にとどまっていること。三つ目に、攻撃者が内部ネットワークに侵害した際、マルウェアの使用を減らして正常プログラムの LOLBins を活用したためだ。

LOLBins は『Living Off the Land Binaries』の略で「自給自足」の意味をもつ。この用語は 2013年頃から言及された。LOLBins はシステムにインストールされた正常なプログラムが攻撃者の目的のために使われることを意味する。

これらのファイルはほとんど管理目的のプログラムで、プログラム実行、ダウンロード、サービス変更、レジストリ照会及び変更、ADS 活用、スクリプト実行など様々な目的で使用できる。同プログラムはシステムに存在する正常プログラムであるため、アンチウイルス製品が悪性ファイルとして認知しない。

[図 6] LOLBins の例

ラテラルムーブメント、追跡が困難な理由

前述したように APT タイプのインシデントは認知するのも簡単ではないが、ラテラルムーブメントの過程が含まれたインシデントを分析することもまた簡単ではない。その理由は次の通りである。

- ログ不足
- 攻撃者が意図的に痕跡を削除
- インシデント認知の遅れ
- 識別が困難

ラテラルムーブメント行為、特にクライアント PC 間の移動についてはログがあまり残らない。攻撃者はそれすらまた意図的に削除する。最近使用が増加している SSD ストレージもまた削除されたファイルの復元が困難であり、削除によるアンチフォレンジック行為は攻撃者の立場からは非常に有効である。前述したように、インシデントを遅く認知するのも追跡を困難にさせる原因でもある。時間が経つにつれてシステムに残っている痕跡は消えていくためだ。これこそ速やかにインシデントを認知しなければならない理由でもある。別の理由には痕跡が残っているとしても識別が難しいという点がある。システム間ユーザーアカウントを利用した認証及び通信行為は、正常な動作なのか悪意ある動作なのか区別することがとても難しい。インシデント分析は、痕跡を辿って攻撃者の行為を逆追跡することだが、上記のような理由から最近は痕跡だけで攻撃者を追跡するのが難しくなっている。よって痕跡が消えないようにしっかり残すことが非常に重要だ。

ラテラルムーブメントを事前に食い止められるか

ラテラルムーブメントは認証情報、ネットワーク、サービス要素のうち一つでも満たされなければ成功できない。つまり内部ネットワークシステムとサービスにアクセスできるアカウントを露出させなかったり、ネットワークレベルで遮断したり、システムで該当のサービスを提供しないようにすればラテラルムーブメント行為が発生しないようにすることもできる。

まず認証情報を保護する方法について探ってみよう。基本的には各ユーザーが自身のアカウント情報の保管に注意しなければならない。アカウント及びパスワードを平文ファイルで保存したり、メールやメッセンジャーを使ってやりとりしてはならない。セキュリティ部門では各システムがパスワードを安全に運用できるように、複雑度、周期変更、同じパスワード再使用禁止などのパスワードポリシーを設定する必要がある。システム数が多くない組織では、管理者(Administrator)アカウントを管理用途で使う場合、全てのシステムに同じパスワードを使う事例が多いがもし 1台のシステムから管理者アカウントが奪取された場合、システム全体がリスクにさらされることになる。

同じく Active Directory を使用する組織も注意しなければならない。管理者権限の Active Directory のアカウントを利用して別のシステムにアクセスする場合、Mimikatz のようなツールはシステム同士の認証後、メモリ上にキャッシングされて残っている認証情報を狙う。よって認証情報のキャッシュ数を最小化するように設定したり、LSASS メモリ内に平文パスワードが保存されないようにする必要がある。
そのための設定方法は次の通りだ。

- HKLM¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion¥Winlogon レジストリキーの Cached-LogonsCount を 0 または 1に設定
- HKLM¥SYSTEM¥CurrentControlSet/Control/SecurityProviders/Wdigest レジストリキーの Use-LogonCredential を 0に設定 (KB2871997 パッチ後、レジストリ修正)

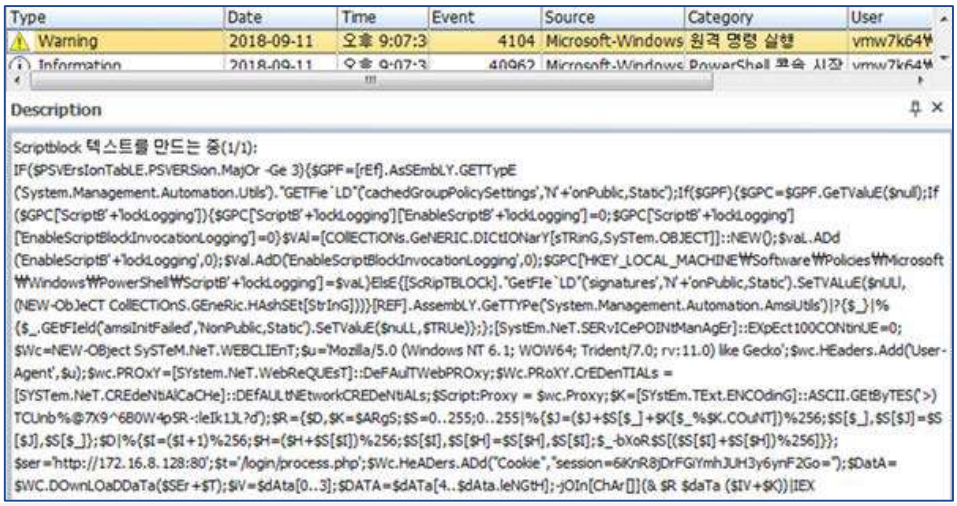
また管理者権限をもつアカウントで別のシステムにアクセスした後は、該当のシステムを必ず再起動する必要がある。ネットワークの観点では組織内で重要なシステムはネットワークを分離して運用することが望ましい。部門、用途別に最小単位でネットワークを分離して構成する必要がある。ネットワーク全体がつながっている場合はたった一人のミスによって組織全体がリスクにさらされる可能性があるからだ。
各システムは必要なサービスだけ活性化して使用する。特にファイル共有機能や WMI、RDP 機能などを使わなければ、各システムのサービスをオフにして該当のサービスが使用するポート (TCP 135, 445, 139, 3389, 49154)は遮断するなどの処置が必要である。

ラテラルムーブメント、発生後に認知できるのか

前述したように、ラテラルムーブメントの行為は正常ユーザーの行為と大きく違わない。よって悪性ファイルや悪意ある動作を検知するセキュリティ製品で検知するのは難しい。それを認知できるいくつかの方法を次に提示する。
一つ目に、組織内にハニーポットシステム、或いはアカウントを利用することである。これをモニタリングしていて攻撃者がハニーポットシステムにアクセスしたり、ハニーポットのアカウントが使われた場合はインシデントとして認知する。攻撃者はしっかり管理されない休止システムを狙う場合が多い。逆をとると組織内に残っている休止システムをこのような用途で活用することも可能だ。
二つ目に、機械学習技術を利用して正常プログラムの異常実行の有無を検知することである。ラテラルムーブメントに使用されるプログラムの実行パターン或いはネットワークアクセス履歴を確認し、正常臨界値から逸脱する異常行為が発生した際にインシデントと判断する方式である。勿論組織ごとに正常と異常の範囲が異なるため、組織に見合ったトレーニングシステムが必要となるだろう。日本インシデント対応センター(JP-CERT)では、そのようなアプローチ法でラテラルムーブメントを検知した事例を発表している。
三つ目に、最近ウェブで頻繁に適用される方法を利用することである。例えば認証の際、当事者に携帯の文字メッセージやメールを送信することで、認証の発生が正常ユーザーによるものなのか当事者に確認する方法だ。

ラテラルムーブメント、事後追跡可能か

ラテラルムーブメントを追跡するには十分な痕跡が必要だが、実際はほとんどそうではない。そのためエンドポイントシステムのログ収集及び管理方策を強化する必要がある。ログの保存期間は 2年以上残るように設定し、やむを得ない場合でも最小 6ヶ月は保管しなければならない。該当のログは別途のシステムに保存して攻撃者に削除されないようにする。
ラテラルムーブメント追跡に必要なログは、Windows で基本的に提供する Security.evtx だ。同ログにはシステムで認証が発生した際にログが残る。またプログラムの実行とネットワークアクセスログが必要だが、これは Microsoft が買収した Sysinternals で無料提供する Sysmon ツールを利用して簡単に確保できる。また PowerShell の場合、4.0バージョンからサポートされるスクリプトブロックのログ記録を有効にすればシステムで実行される PowerShell スクリプトを確保できる。最近はエンドポイントの行為情報を収集する EDR ソリューションが多く登場しており、これらのソリューションが活用される場合もある。



[図 7] Microsoft-Windows-PowerShell/Operational.evtx

APT 攻撃の特性上、インシデントを 100% 遮断することはできない。攻撃者が組織のユーザー PC を侵害するのに成功した以降は、内部ネットワークで使用されるアカウント情報を獲得しようとし、それによって内部ネットワークをあれこれ見回るようになる。この際に攻撃者はマルウェアの代わりに正常プログラム(LOLBins)を使用するため管理者に検知されにくい。

これらの情報をもとに、管理者は外部からの脅威ではなく既にアカウントを知っている内部ユーザーを攻撃者に想定して内部セキュリティポリシーを検討しなければならない。特に最近はエンドポイントを侵害した後に内部ネットワークを移動する方法が主に使われるため、エンドポイントで発生する行為をしっかり観察して脅威ハンティング(Threat Hunting)活動を積極的に実施すべきである。

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)