アンラボ・セキュリティレター

Press Ahn

2020.10　Vol.82

ハッカーの強力な武器、ファイルレス攻撃とは

犯罪の痕跡を残さないファイルレス攻撃の増加

ハッカーの強力な武器、ファイルレス攻撃とは

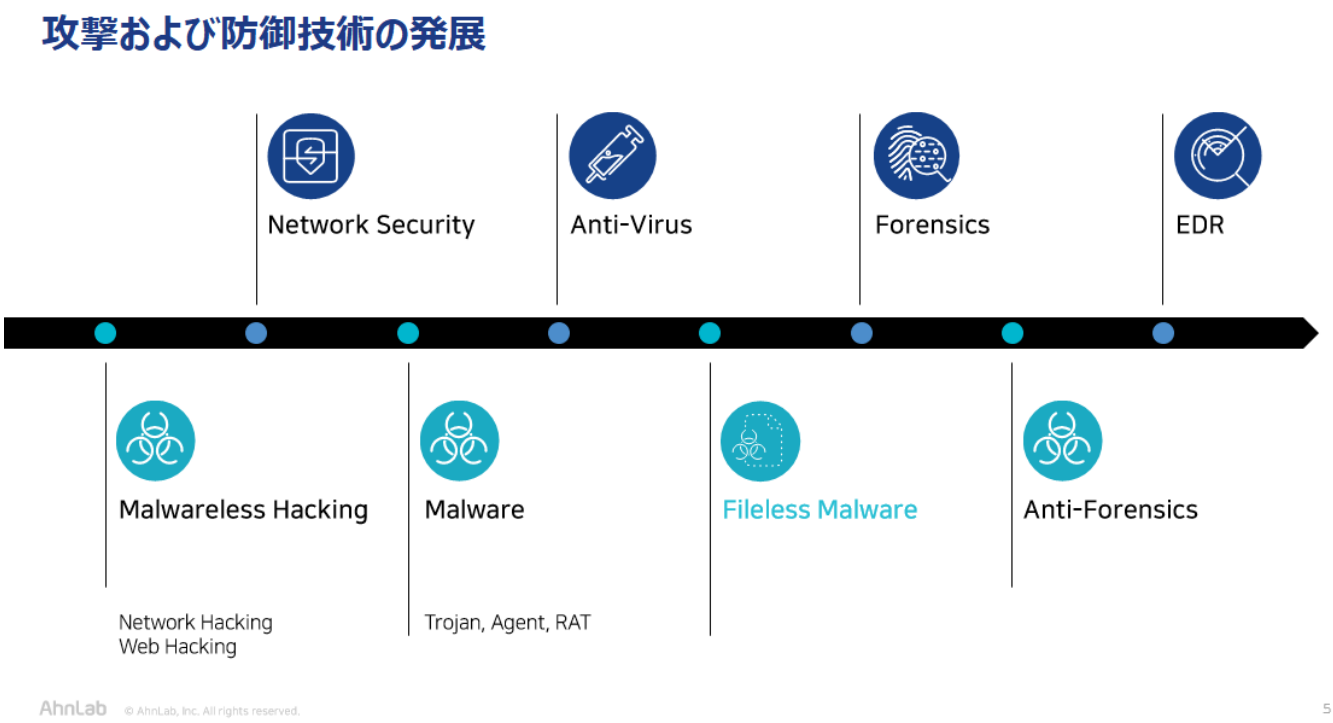
数年前から「ファイルレス(fileless)」という言葉がセキュリティ脅威レポートや関連ニュースに度々登場している。グローバル情報セキュリティ企業のトレンドマイクロ(Trend Micro)は、昨年に発刊した「2019中間セキュリティ脅威レポート」を通して2019年上半期に検知されたファイルレス攻撃の件数が2018年同期に比べて、265%以上増加したと明かした。アンラボも今年に発表した「2020セキュリティ脅威の見通し」で、ファイルレス方式のターゲット型ランサムウェア攻撃について予測したことがある。このように、セキュリティ企業が持続的な増加を見通しているファイルレス攻撃とは何だろうか？

今回はファイルレス攻撃の定義と発展過程について紹介する。

ファイルレス攻撃は、「有害な機能を遂行するコードをメモリ内でのみ実行させ、システムに被害を与えるタイプの攻撃」を意味する。攻撃者がファイルレス手法を使用してもディスクに何も残さないわけではない。攻撃者は攻撃の持続性(persistence)を維持するためにマルウェアを保存媒体に保存する必要がある。ただ、この場合、攻撃者は我々が知っている実行ファイル、スクリプトファイル、文書ファイルのような個別ファイルでは保存しない。つまり、保存媒体にはファイル形式のマルウェアが存在しないことだ。

ファイルレス攻撃の出現と発展

ファイルレス攻撃の出現背景と攻撃、防御技術の流れについて簡単に調べてみる。



[図1] ファイルレス攻撃&防御技術の発展

サイバー攻撃手法にはマルウェアを使用しない攻撃も多く存在する。特にネットワークやウェブを通した攻撃はマルウェアがなくても可能な場合が多い。このような種類のネットワーク攻撃はファイアウォール、ウェブアプリケーションファイアウォール、侵入検知システム(Intrusion Detection System, IDS)などのネットワークセキュリティ装備を活用して防御する。

攻撃者はネットワークを通した直接的なアクセスが難しい場合、メールの添付ファイルやインターネットを通して感染ファイルを流入させる方法を選択できる。防御する立場ではこのような感染ファイルを検知、ブロック、削除するため、いわゆるウイルス対策プログラムと呼ばれるAV(Anti-virus)ソリューションを使用する。AV ソリューションは主にファイルを対象に動作する。攻撃者はAVを回避するために様々な手法を使用できるが、そのうちの一つがファイルを使用せずにマルウェア、つまりファイルレスマルウェアを活用することである。

脅威分析専門家たちはマルウェアが AV に検知されなくても、フォレンジック(forensic)技法を活用して、さらなる脅威を探し出し、または攻撃者の流入ルートなどの攻撃情報を把握することができる。攻撃者はフォレンジック技法を利用した追跡を避けるために、できる限り痕跡を消す。このような攻撃者の行為をアンチフォレンジック(Anti-forensic)と言う。

ファイル、またはシステム上の痕跡を分析することが段々難しくなり、2015年頃からはセキュリティ市場には感染ファイルでない行為に集中するEDR(Endpoint Detection and Response)タイプの製品が登場し始めた。

ファイルレス攻撃が話題になる理由

ファイルレス攻撃が最近登場した攻撃手法でないにも関わらず、最近になって話題になる理由は何だろうか？

一つ目は、ファイルレス攻撃にパワーシェル(PowerShell)が用いられて以降、APT(Advanced Persistent Threat)攻撃やランサムウェア、仮想通貨マイナーなどのマルウェア配布まで、全方位的に拡散しているからである。特に、パワーシェル基盤のファイルレス攻撃機能を搭載した様々な攻撃シミュレーションツールが公開されており、技術的に接することも比較的にしやすい。最近、発生した侵害事故から該当ツールを使用した痕跡が少なからず発見されている。

二つ目は、ファイルレス攻撃がエンドポイントセキュリティ市場の「ゲームチェンジャー」の役割をしていることである。ファイルレスマルウェアはファイルに焦点を合わせた既存のセキュリティソリューションでは検知が難しいため、これを解決するために登場したEDRの市場形成と成長を促進させると言える。

これからは AVT(Advanced Volatile Threat)？

APT 攻撃は、訳すと「知能型の持続的な脅威」と言える。最近、APT 攻撃が敢行された侵害事故でファイルレス攻撃が多く発見されているが、これに因んで APT を AVT、つまり知能型の揮発性脅威(Advanced Volatile Threat)と呼ぶこともある。

AVT 攻撃はファイルレス手法が使用されるのだが、攻撃者はメモリ内でのみ動作するインメモリマルウェア(in-memory malware)と LOL ツールを使用し、ターゲットシステム内に有害な痕跡をできる限り残さないようにしている。LOL ツールは「Living Off The Land」の略語で、自給自足という意味である。攻撃者が攻撃過程で外部ツールではなく、対象のシステム内の正常なツールを使用するという意味で理解していいだろう。

ファイルレス攻撃のデータ保存場所

攻撃者は意図的にディスクに攻撃データを全く残さずに攻撃を遂行することができる。その際、マルウェアはメモリ内でのみ存在することになる。ただ、この場合はシステムが再起動するとマルウェアがすべてなくなり、ターゲットシステムの制御権をまた得るためにもう一度攻撃を遂行しなければならないという負担がある。特別な場合を除いて、攻撃者がこのような戦略を選択することはあまりない。

そのため、ほとんどの攻撃者はターゲットシステムが再起動しても、マルウェアが持続的に動作して制御権を維持できる持続(persis

tence)戦略を選択する。このために最小限のマルウェアをシステムに残しておく。よく選ばれる場所はレジストリ、サービス、タスクスケジューラ、WMI(Windows Management Instrumentation)など、OS で提供している領域である。その他、一般的ではないが、ユーザーのアプリケーションのデータベースのような場所、ディスクファイルシステムの外部、未使用のスラック領域、HDDのファームウェアなど、OS 管理領域以外の場所にも保存できる。

攻撃者がファイルレス手法を使用する理由

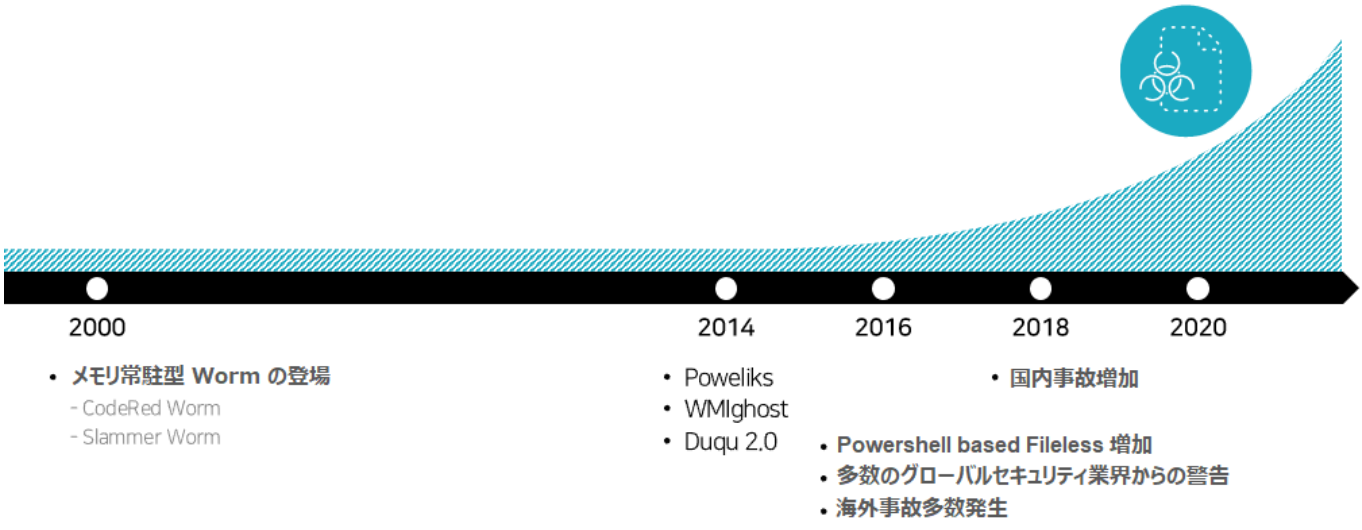
攻撃者がファイルレス手法を使用する理由は攻撃を検知・追跡されたくないからである。

まず、検知回避の観点からみると、攻撃者が流入させたマルウェアがディスク内にファイル形式で存在しない場合、スキャンする対象がないため、AV ソリューションに検知されない。また、ホワイトリストプロセスのみ動作できるように制御するセキュリティソリューションにも LOL ツールとともにファイルレス手法が使用されれば、正常に見えるため制裁なく実行可能となる。

追跡回避の観点からもセキュリティ担当者が確認するファイルがないとファイルハッシュを求めることができない。それでは、脅威情報(Threat Intelligence)を得るためにウイルストータル(Virus Total)などのサイトで照会する場合、どうすればいいだろう。結局、マルウェアや攻撃者を識別して判断するための情報が不足するため、攻撃者の立場としては感染ファイルを使用しない方が有利だ。攻撃者はディスクに攻撃に関する情報の保存を最小化し、保存された場合は完全削除などを通して追跡の手がかりになるものを無くす努力をする。

ファイルレス攻撃の登場と増加

前述したように、ファイルレス攻撃は最近登場した手法ではない。2000年代にもメモリ常駐型マルウェアが存在しており、その後も類似したマルウェアが引き続き登場した。以降2016年、パワーシェルが使用されるようになってからファイルレス攻撃は増加傾向を示した。2018年から韓国でもパワーシェル基盤のファイルレス手法を使用した侵害事故が確認され始めた。



[図2] ファイルレス攻撃の変化

ファイルレス手法を使用する攻撃グループ

マイターアタック(MITRE ATT&CK)ではファイルレス手法を別途の戦術(tactic)や技術(technique)として区別していない。しかし、パワーシェルや関連ツールの使用有無などを通し、ファイルレス手法を使用した攻撃グループを特定することは可能だ。マイターアタックは様々なセキュリティ企業や公共機関、個人が発行した公開レポートや資料を分析して知られた攻撃グループに関する情報をまとめて公開している。マイターアタックで公開した94個の攻撃グループを分析した結果、ファイルレス手法を使用したと推定されるグループは約40%(35個)に至る。

admin@338, APT1, APT3, APT12, APT16, APT17, APT18, APT19, APT28, APT29, APT30, APT32, APT33, APT37, APT38, APT39, APT41, Axiom, BlackOasis, BRONZE BUTLER, Carbanak, Charming Kitten, Cleaver, Cobalt Group, CopyKittens, Dark Caracal, Darkhotel, DarkHydrus, Deep Panda, Dragonfly, Dragonfly 2.0, DragonOK, Dust Storm, Elderwood, Equation, FIN10, FIN4, FIN5, FIN6, FIN7, FIN8, Gallmaker, Gamaredon Group, GCMAN, Gorgon Group, Group5, Honeybee, Ke3chang, Kimsuky, Lazarus Group, Leafminer, Leviathan, Lotus Blossom, Machete, Magic Hound, menuPass, Moafee, Molerats, MuddyWater, Naikon, NEODYMIUM, Night Dragon, OilRig, Orangeworm, Patchwork, PittyTiger, PLATINUM, Poseidon Group, PROMETHIUM, Putter Panda, Rancor, RTM, Sandworm Team, Scarlet Mimic, Silence, SilverTerrier, Soft Cell, Sowbug, Stealth Falcon, Stolen Pencil, Strider, Suckfly, TA459, TA505, Taidoor, TEMP.Veles, The White Company, Threat Group-1314, Threat Group-3390, Thrip, Tropic Trooper, Turla, Winnti Group, WIRTE

[図3] ファイルレス手法を使用したと推定される攻撃グループ

パワーシェル基盤のファイルレス手法が使用された主要攻撃事例

2016年米DNC(民主党全国委員会)ハッキング事件

2016年、米大統領選挙の当時、ロシアと推定される攻撃者が民主党の組織をハッキングした事件があった。当時、米国のセキュリティ企業クラウドストライク(Crowdstrike)から2週間行われたフォレンジック分析の結果が発表されたが、現在も攻撃者について法的攻防が進行している。このような有名な事件にパワーシェルワンライナー(PowerShell One-liner)を WMI に登録する手法が使用された。パワーシェルワンライナーに関する詳しい内容は後述する。

2017年全世界40か国で140個の組織がハッキングされた事件

カスペルスキーは2017年、全世界40か国の政府、金融、通信など、約140個の組織が類似した手法の攻撃に侵害されたという報告書を公開した。この攻撃はパワーシェルワンライナーをレジストリやサービスに登録する方法が使用された。

2018年~現在 : ランサムウェア配布方式の変化

2018年からは既存のドライブバイダウンロード(Drive-By-Download)、正常ソフトウェア偽装、メール添付などの方法で配布された有名ランサムウェアがファイルレス手法を使用して拡散し始めた。アンラボがASECのブログを通して公開したランサムウェアの変化の推移は下記の通りだ。

作成日	タイトル
2018/04/17	ファイルレス手法で拡散する GandCrab v2.1
2018/06/05	ファイルレス手法の Magniber ランサムウェアの再登場

2018/07/06	パワーシェルスクリプトを利用した GandCrab ランサムウェアの拡散(ファイルレス)
2018/08/29	JavaScript 内に含まれた GandCrab ランサムウェア (V3 除去を誘導)
2018/09/03	パワーシェルを利用して拡散中の GandCrab v4.4 (Kill-Switch)
2018/10/01	WMIC を利用した V3 Lite 除去機能の GandCrab v5.0.1 登場
2018/10/29	[注意] 不復元 GandCrab v5.0.4 韓国内で拡散中
2018/11/16	SEON ランサムウェアの注意(ファイルレス手法)
2019/09/06	ファイルレス手法で動作する WannaMine (SMB脆弱性)
2019/12/03	SMB 伝播機能である Lemon_Duck マルウェアの拡散
2019/12/17	ファイルレス手法の BlueKeep の脆弱性 V3行為検知の動画
2019/10/11	[注意] 文書形態で拡散するエモテット(Emotet)マルウェア
2020/02/14	IE 脆弱性(CVE-2019-1367)に対するV3行為検知(ファイルレス手法)

[表1] ランサムウェアの変化の推移

2019年韓国の大企業、MyKings ボットネット感染

2019年には韓国の大企業の一か所が、MyKings というボットネットに感染する事件が発生した。攻撃者の目的は仮想通貨発掘マルウェア(CoinMiner)を動作させることだった。攻撃者は多数のシステムを感染させるため、EternalBlue の脆弱性を利用し、パワーシェルワンライナーをタスクスケジューラとサービスに登録させる方法も並行した。

2019年 CLOP ランサムウェア感染

昨年は韓国内400個以上の組織を感染させた CLOP ランサムウェア事件で、セキュリティ業界が騒がしかった。CLOP ランサムウェア攻撃は APT とランサムウェアが合わさったタイプだった。攻撃者は Cobalt Strike という攻撃シミュレーションツールを使用し、ファイルレス観点ではパワーシェルワンライナーをサービスに登録する手法が使用された。

効果的な防御のためには優れたソリューションと防御者の自発的努力が必要

2016年以降、パワーシェルを利用したファイルレス手法はAPT攻撃やマルウェア配布など、ウィンドウシステムを掌握するための効果的な方法として使用されている。攻撃者は200バイト程度の短いパワーシェルワンライナーだけでメモリ内でのみ動作するマルウェアを駆動させることができる。さらに、制御権を持続的に維持するためにバックドアを仕込んだり、パワーシェルワンライナーをファイルではないかたちでディスクに保存したりもする。

ファイルレス攻撃はファイルを使用しないため、一般的な AV ソリューションでは対応が難しい。攻撃者の行為を把握するためには

システムのロギングを強化し、持続的に検討する必要がある。攻撃者の行為は明確に悪性と判断しにくい方法へと徐々に進化しているため、このような観点から EDR ソリューションの活用が適切な選択と判断される。

攻撃者は常に既存の防御システムを迂回できる方法を見つけることに成功してきた。このような攻撃者を阻止するために新たな検知技法が追加され、対応方法を向上させるなど、防御システムも発展している。しかし、攻撃と防御の戦争は終わらない。攻撃手法が登場し、防御技法が追いつく時間差を克服するためには、セキュリティのソリューションに頼るだけでなく防御者自ら新たな攻撃技術に関心を持つ努力が必要である。

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)