2017年に登場したランサムウェアMagniberが2021年に復活、脆弱性PrintNightmareを利用して韓国のユーザーに感染

August 11, 2021 | Liviu Arsene | エンドポイントとクラウドのセキュリティ

- 2017年のランサムウェアMagniberが復活し、韓国のユーザーに対してパッチ未適用の脆弱性を狙うという以前の手法が再び用いられている
- 2021年7月、CrowdStrikeはランサムウェアMagniberが既知の脆弱性PrintNightmareを利用して侵害を試みていることを特定
- CrowdStrikeは、PrintNightmareの悪用と、Magniberランサムウェアの攻撃の両方の検知・防御が可能

CrowdStrikeは最近、2017年に活動していたランサムウェアファミリー Magniberが関与する新たな活動を確認しました。この活動では韓国の被害マシン上で、**PrintNighmareの脆弱性**が悪用されました。7月13日、CrowdStrikeはPrintNightmareの脆弱性の悪用を阻止し、データが暗号化される被害を受ける前に顧客を保護しました。

PrintNightmareの脆弱性（**CVE-2021-34527**）が公開されたとき、CrowdStrike Intelligenceは、この脆弱性によってリモートコード実行（RCE）やローカル権限の昇格（LPE）が可能になるため、攻撃者に利用される可能性が高いと判断しました。今回のインシデントでは、この判断が正しいことが証明されました。

エンドポイントを侵害するために攻撃者が用いる戦術や技術に対する緩和策を講じながら、CrowdStrike Falcon®プラットフォームは、センサー上とクラウド内での機械学習および攻撃の痕跡（IOA）データを活用して、既知あるいは未知の脅威が関与する悪質なプロセスやファイルを特定し、脅威に対する多層的な防御機能を提供します。

脆弱性PrintNightmareに関するタイムライン

2021年6月8日：PrintNightmareの脆弱性（**CVE-2021-1675**）は、6月8日に、3つの異なる企業で働くセキュリティ研究者達によって発見され、マイクロソフトに報告されました。彼らは、以前に提供されたPrintDemonの脆弱性（CVE-2020-1048）のパッチを回避する研究を行っていました。

2021年6月21日：マイクロソフトは、**2021年6月のセキュリティ更新プログラム**の中で、**CVE-2021-1675**のパッチを公開しましたが、脆弱性の悪用手口に関する追加情報は公開されませんでした。当時、この脆弱性は、ローカルで認証されたユーザーでなければ悪用できないと考えられていました。しかし、この脆弱性がリモートコードの実行を可能にする可能性があると判断されたため、マイクロソフトは6月21日に、この脆弱性の重大度を「Critical（危険）」に修正しました。

2021年6月29日：これとは別に、Windows Print Spoolerサービスの同様のバグを調査していた3人のセキュリティ研究者のうちの1人が、6月29日にこの脆弱性（**CVE-2021-1675**）の概念実証（POC）コードを、GitHubのリポジトリで誤って公開してしまいました。この誤りはすぐに修正されたものの、このGitHubリポジトリはコピーされ、POCが流出してしまい、攻撃者らに悪用される可能性が生じました。

2021年7月1日：マイクロソフトは、**CVE-2021-1675**の脆弱性に対するパッチを発行したものの、流出したPOCコードでPrint

Spoolerの脆弱性を狙った別の攻撃ベクトルが使用され、7月1日にこの脆弱性を悪用する複数のPOCが公開されました。そのため、7月1日にマイクロソフトは2つ目のCVE（**CVE-2021-34527**）を発行し、「CVE-2021-1675は、CVE-2021-34527と類似しているが別物である」と発表しました。

2021年7月6日：7月6日、マイクロソフトは、**CVE-2021-34527**の脆弱性修正のための**OOB（累積更新）**アップデートを公開しました。しかし、その数時間後、セキュリティ研究者達が、特定の条件下においては、修正プログラムも回避可能であることを発見しました。攻撃者らは、MetasploitやMimikatzなどの人気のあるエクスプロイトツールに**このエクスプロイトコードを組み込み**、まだパッチが適用されていないこの脆弱性の利用を容易にしました。

ランサムウェアMagniberとは

Magniberランサムウェアは、2017年後半に、韓国の被害者を標的としていたことが最初に確認されました。この攻撃者らは、Magnitudeエクスプロイトキットを使用したマルバタイジング（不正広告）攻撃でMagniberを使用していました。Magniberを使用した以前の攻撃では、韓国のユーザーのみが狙われていましたが、2018年半ばには、他のアジア太平洋諸国のユーザーも標的とされました。

当初、Magnitudeエクスプロイトキットのオペレーターは、ランサムウェアCerberのみを使用していましたが、その後、その後継とされるMagniberに乗り換えています。Magniberの最も一般的な感染ベクトルでは、パッチ未適用の脆弱性、たとえば、Internet Explorerの脆弱性（**CVE-2018-8174**、**CVE-2021-26411**、**CVE-2020-0968**、**CVE-2019-1367**）あるいはFlashの脆弱性（**CVE-2018-8174**）を悪用し、危険なWebサイトやドライブバイダウンロードを介して感染させていました。

2017年から活動していたランサムウェアMagniberは、韓国人のみをターゲットとしているように見えました。Falcon OverWatch™チームは、2021年2月初旬にもMagniberによる活動を検知しています。Magniberは、Internet Explorerの脆弱性（CVE-2020-0968）を悪用して韓国のユーザーのみを攻撃していました。

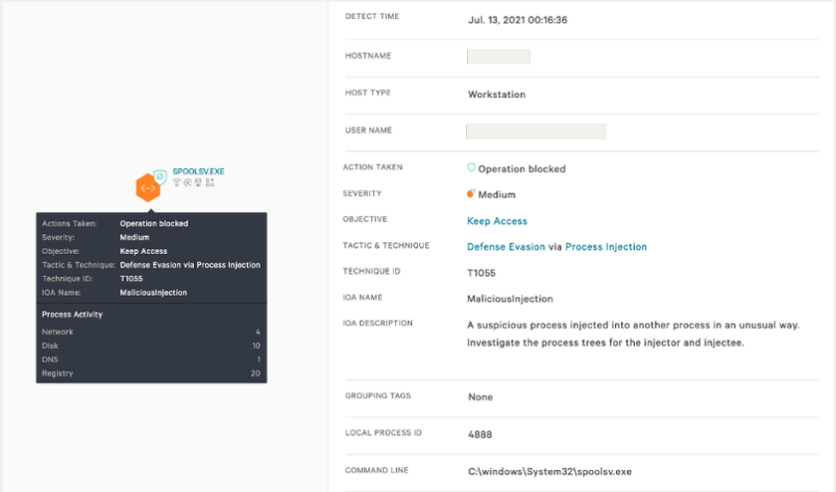
このランサムウェアは、積極的に開発され続けており、新たな難読化機能、検出回避技術、暗号化強化メカニズムを組み込みながら、長年にわたって散発的に利用されていました。この開発者らは、感染をアジア太平洋地域内に留めようと、さまざまな言語チェック機能を盛り込みました。

PrintNightmareとランサムウェアMagniberとの出会い

最近のPrint Spoolerの脆弱性、PrintNightmareを利用したMagniberランサムウェアの新たなインシデントは驚くべきことですが、この脆弱性がもたらす影響を考えれば珍しいことではありません。この問題が報告されてから、複数のPOCが公開されたため、攻撃者らがこれを悪用してユーザーを侵害し、悪質なペイロードを送り込むのは時間の問題でした。

Falcon OverWatchチームは、PrintNightmareの脆弱性を悪用しようとする動きを継続してハンティングしており、最近、ある挙動に気づきました。悪質なDLLが「\Device\HarddiskVolume2\Windows\System32\spool\DRIVERS\x64\3\New\」フォルダに書き込まれ、その後「spoolsv.exe」プロセスにロードされていました。このDLLは、ランサムウェアMagniberに関連するもので、ランサムウェアのコアDLLの難読化解除を行い、リモートプロセスにインジェクションする役割を担っています。

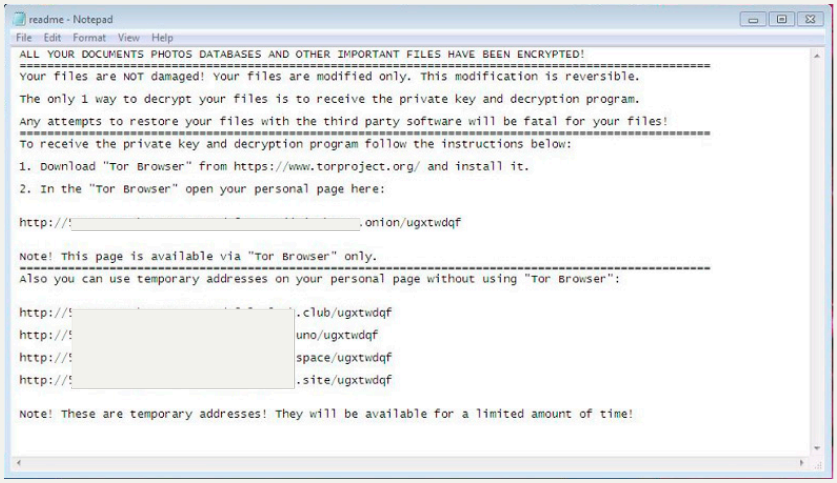
PrintNightmareの調査の一環としてリリースしたIOAのカバレッジにより、次のスクリーンショットに示すように、このアクションが正しく検知され、オペレーションがブロックされていることが分かります。



IOAを用いたCrowdStrikeのふるまいベースの検知機能によって、ランサムウェアのコアDLLのインジェクションを防ぐことに成功し、エンドポイント上で暗号化が行われる前に悪質なアクティビティを阻止しました。

悪質なランサムウェアサンプルのふるまい分析を行うと、CrowdStrikeのセキュリティ研究者が過去に観察したMagniberのふるまいと一致することがわかりました。つまり、脆弱性を悪用して、難読化されたDLLローダーをドロップし、そのローダーをプロセスに注入して、ローカルファイルのトラバーサルと暗号化を行うコアDLLローダーを解凍するという、既知のMagniberと同様の手口が用いられていました。

ドロップされた身代金メモからは、このインシデントの首謀者や身代金の支払い額についての新情報は得られていません。メモには、ランサムウェアのオペレーターに連絡して交渉するようにと書かれており、リンクが切れる制限時間までに、データ復号化の手続きをとるようにと警告しています。



CrowdStrike Falconによる保護

CrowdStrike Falconは、機械学習とふるまいベースの保護機能を駆使し、組織にとって最も価値のあるエンドポイントの保護を実現する階層型アプローチを採用しています。Windows Print Spoolerの重大な脆弱性であるPrintNightmareは、すべてのWindowsホストに影響を与える可能性があります。そのため、CrowdStrikeのお客様には、ベストプラクティスに基づいて防御ポリシーを見直したうえで、Falcon Spotlight™による脆弱性管理を実施し、関連するリスクを特定することをお勧めしています。**Falcon Spotlight** を導入されていないお客様も、無料のトライアルをご利用いただけます。

新しい未知の脅威に対処する際にも、CrowdStrike Falconは、機械学習とIOAを活用して、悪質なプロセスやファイルの挙動を特定します。**このビデオ**では、MagniberランサムウェアのDLLを正常に検知してブロックするFalconの機能を紹介しています。まず、Magniber DLLがディスクに書き込まれた時とリモートプロセスに注入された時に、Falconがいかにしてクラウドベースの機械学習を使用して、Magniber DLLを検知しているかをご覧ください。Falconがベストプラクティスに基づいてすべての防御・保護ポリシーを有効化して、Magniberランサムウェアをブロックするデモもご覧ください。Falconセンサーがただちに Magniberの悪質なふるまいをブロックし、エンドポイントを保護します。

CrowdStrikeは、160以上の特定済みの攻撃者グループに加え、多数の無名のグループや脅威に関連するTTP（ 戦術、テクニック、手順）を継続的に監視し、その情報をFalconプラットフォームにフィードしています。

CrowdStrikeでは、PrintNightmareの脆弱性とランサムウェアの組み合わせが、今後も他の攻撃者らによって悪用される可能性が高いと予測しています。皆様には、常に最新のパッチやセキュリティアップデートを適用して既知の脆弱性に対応するとともに、セキュリティのベストプラクティスを遵守することで、脅威や高度な敵に対するセキュリティ体制を強化することをお勧めします。

攻撃の痕跡（IOC）

ファイル	SHA256
Magniber Loader DLL	10b9b1d8f6bafd9bb57ccfb1da4a658f10207d566781fa5fb3c4394d283e860e 36417f0ea6d948cbd7e003b3cefbb603d886849a8c80e0999c7969b03f2b9c28 66c4f54da6542339de036872e80306f345b8572a71e782434245455e03541465 77d3b1cf6d5a0a07090cdb078dce6e3849465c9acde7e1ba66c3893fefc73d4b 9a6584a163d8c378e6f873c5544794274cce2532e91fc079b79fd73399447b03

その他のリソース

- Falcon Spotlightが、お客様の組織における脆弱性の発見と管理にどのように役立つかをご紹介します。
- Falcon SpotlightとFalcon Real Time Response（RTR）を使用して緊急パッチの適用を実施する方法をご覧ください。
- CrowdStrike Falcon Identity ProtectionソリューションのWebページをご一読ください。
- CrowdStrike Falcon Zero TrustおよびFalcon Identity Threat Detectionのデモのご用命を承っております。

原文：Teaching an Old Dog New Tricks: 2017 Magniber Ransomware Uses PrintNightmare Vulnerability to Infect Victims in South Korea
https://www.crowdstrike.com/blog/magniber-ransomware-caught-using-printnightmare-vulnerability/