ホワイトペーパー

ランサムウェアバイナリの実験に基づく比較分析

Shannon Davis著

SURGe by Splunk

splunk> turn data into doing

概要

セキュリティ研究者やネットワーク防御の専門家がランサムウェアについてさまざまな情報を発信しているにもかかわらず、多くの組織は今でもランサムウェア攻撃に先手で対応できず後れを取っています。その原因の一部は、ランサムウェアについてのエビデンスに基づく正しい知識が不足していることにあります。ランサムウェアの暗号化速度は、詳細に研究する価値のあるテーマの1つです。現時点でこのテーマについて最も包括的な情報を公表しているのは、LockBitランサムウェアの作成者自身です。LockBitを生み出した犯罪グループは、著名なランサムウェアファミリーの暗号化速度の比較結果を自らのWebサイトで公開し、LockBitが「最速」であることをアピールしています。このホワイトペーパーでは、これまで犯罪者の手に委ねられていた研究テーマに光を当てたいと思います。私たち調査グループは、管理された環境下で科学的な方法を用いて、10種類の主要なランサムウェアによる暗号化の速度を測定しました。搭載するWindowsオペレーティングシステムとハードウェアの仕様が異なる複数のホストで、約10万個、合計約53GBのファイルを暗号化し、かかった時間を計測しました。私たちはこの実験を通じて、ブルーチームがランサムウェアに対する知識を深め、Lockheed Martin社によるサイバーキルチェーンで言うところの「目的実行」段階ではなく、もっと早い段階で攻撃を検出してより効果的な対策を自信を持って実行できるようになること(Left of Boom)を期待しています。

実験では、ランサムウェアの暗号化速度を測定するためにSplunk Attack Rangeで専用のラボ環境を構築し、4種類のホストと、10種類のランサムウェアのサンプル10個ずつを用意しました。ホストのオペレーティングシステムは、2つがWindows 10、あとの2つがWindows Server 2019です。ランサムウェアサンプルがどのファミリーに属すかは、VirusTotalでのMicrosoft Defender Antivirusの検出結果によってのみ判断しました。プロセッサ、メモリー、ハードドライブ構成の違いによるランサムウェアの動作の変化を検証するために、各ホストには「高」または「中」レベルのリソースを割り当てています。各ホストではWindowsログ機能を有効にして、Splunkでデータを収集、統合、分析します。これらの準備を経て、各種のランサムウェアが約10万個のファイルを暗号化する速度を測定するとともに、プロセッサ、メモリー、ディスクなどのシステムリソースが暗号化速度にどう影響するかを調べました。

100個のランサムウェアサンプルすべてを検証した結果、暗号化にかかる時間(TTE：Total Time to Encrypt)は4分～ 3時間半とサンプルによって差があり、全体の中央値は42分でした。つまり組織は、暗号化が完了するまでのこの限られた時間内に効果的に対応する必要があるということです。リソースが異なるシステム間で同じランサムウェアサンプルの結果を比べると、プロセッサの速度やCPUのコア数など、一部のリソースがTTEに影響することもわかりました。ただし、その差は一貫していないことから、一部のランサムウェアはシングルスレッドにしか対応していないか、リソースが増えても影響は最小限にとどまると考えられます。すべてのシステムで暗号化が最も速かったのはLockBitランサムウェアです。これは、LockBitが各ファイルを4KB分だけ暗号化することでファイルを使用不能にし、効率的に攻撃を行うという既存の報告を裏付けています。また、LockBitの作成者が自らのTor Webサイトで誇示している「最速のランサムウェア」という称号の正しさも証明しています。

SURGeは今後、この調査の結果を基にランサムウェアの全体像を明らかにし、ネットワーク防御に役立つ情報を公開していく計画です。特に、複数のランサムウェアサンプルのファイルアクセス技法を、stoQなどのオープンソースのファイル分析フレームワークツール、ファジーアルゴリズム、SplunkのMachine Learning Toolkit (MLTK)を使って深く掘り下げたいと思います。さらに、最近のランサムウェアは検知を回避するためにパッカーを使用しないという説を検証し、まだ分類されていない未知のランサムウェアバイナリを、実行後の検出時点ではなく「デプロイ」された時点でクラスタリングできるかどうかも調査する考えです。この調査のデータセットは、2022年6月に開催される.conf22で発表する予定です。セキュリティ研究者の方はぜひこの資料を精査し、調査結果を検証して、世界のブルーチームコミュニティの支援にお役立てください。

主な調査結果

- LockBitランサムウェアは、調査対象となった10種類のランサムウェアの中で最速を記録しました。これは、LockBitを作成した犯罪グループが自らのサイトTorで誇示している主張と一致します。
- ランサムウェアが、98,561個、合計で53.83 GBのファイルすべてを暗号化するのにかかった時間の全体の中央値は、42分52秒でした。
- 暗号化の速度は、4分から3時間30分まで、各ランサムウェアのサンプルによって大きく異なりました。
- 一部のランサムウェアサンプルでは、ハードウェアの性能が高くなると暗号化の速度が上がりました。その他のサンプルでは、リソースの性能を十分に活かせず、場合によっては高仕様のシステムでむしろパフォーマンスが下がることもありました。どのサンプルでも、メモリーの量は暗号化の速度にほとんど影響しませんでした。ディスクの速度が上がると暗号化の速度も上がるケースがありましたが、多くの場合、その効果があるのはCPUコア数を増やすと速度が上がるサンプルでした。

はじめに

Mandiant社は2021年度M-Trendsレポートで、2020年に行った調査の25%にランサムウェアが絡んでおり、2019年の14%から増加したと述べています[1]。また、Verizon社は2021年度データ漏洩/侵害調査報告書(DBIR)で、2019年から2021年にかけてランサムウェアの出現頻度が2倍になったと指摘しています[2]。ランサムウェアは世間一般では比較的新しいと思われていますが、初めて確認されたのは1989年のAIDS会議で、フロッピーディスクを介して広がり世界を悩ませました[3]。

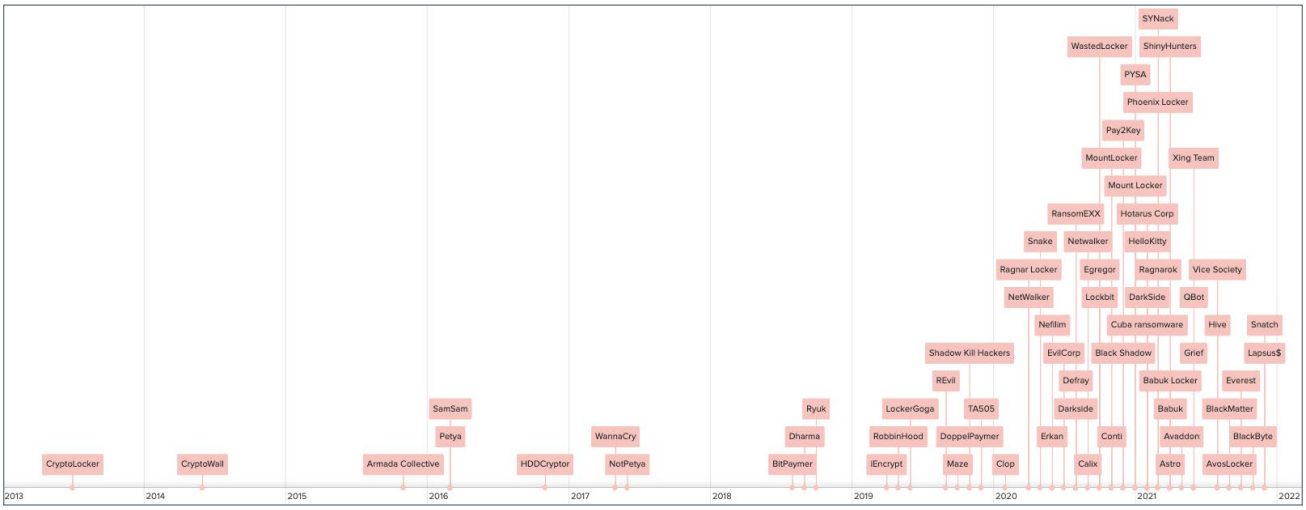

図1：2013年～ 2022年のランサムウェアファミリーの増加状況(Spunk提供)

前述のM-Trendsレポートによると、米国でのランサムウェアの滞留時間の中央値は3日です[4]。3日間の滞留は望ましいとは言えませんが、これまで滞留時間は数時間、人によっては数分であると考えられていました。数時間ではなく数日であれば、対策を取るのにある程度余裕ができます。CERT NZは2021年、ランサムウェアのライフサイクルと、高まる脅威に対抗するために役立つ推奨事項をまとめたホワイトペーパーを公開しています(図2)[5]。

1. FireEye社/Mandiant社、Fireeye-Rpt-Mtrends-2021.Pdf、2021年4月13日、13、https://www.mandiant.com/resources/m-trends-2021
2. Verizon社、DBIR「2021 Data Breach Investigations Report」、2021年5月12日、14、verizon.com/dbir
3. 「Case Study: AIDS Trojan Ransomware」、SDxCentral社、2022年2月23日参照、https://www.sdxcentral.com/security/definitions/case-study-aids-trojan-ransomware/
4. FireEye社/Mandiant社、「M-Trends 2021」、14
5. 「How Ransomware Happens and How to Stop It」、CERT NZ、2022年1月29日参照、https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/

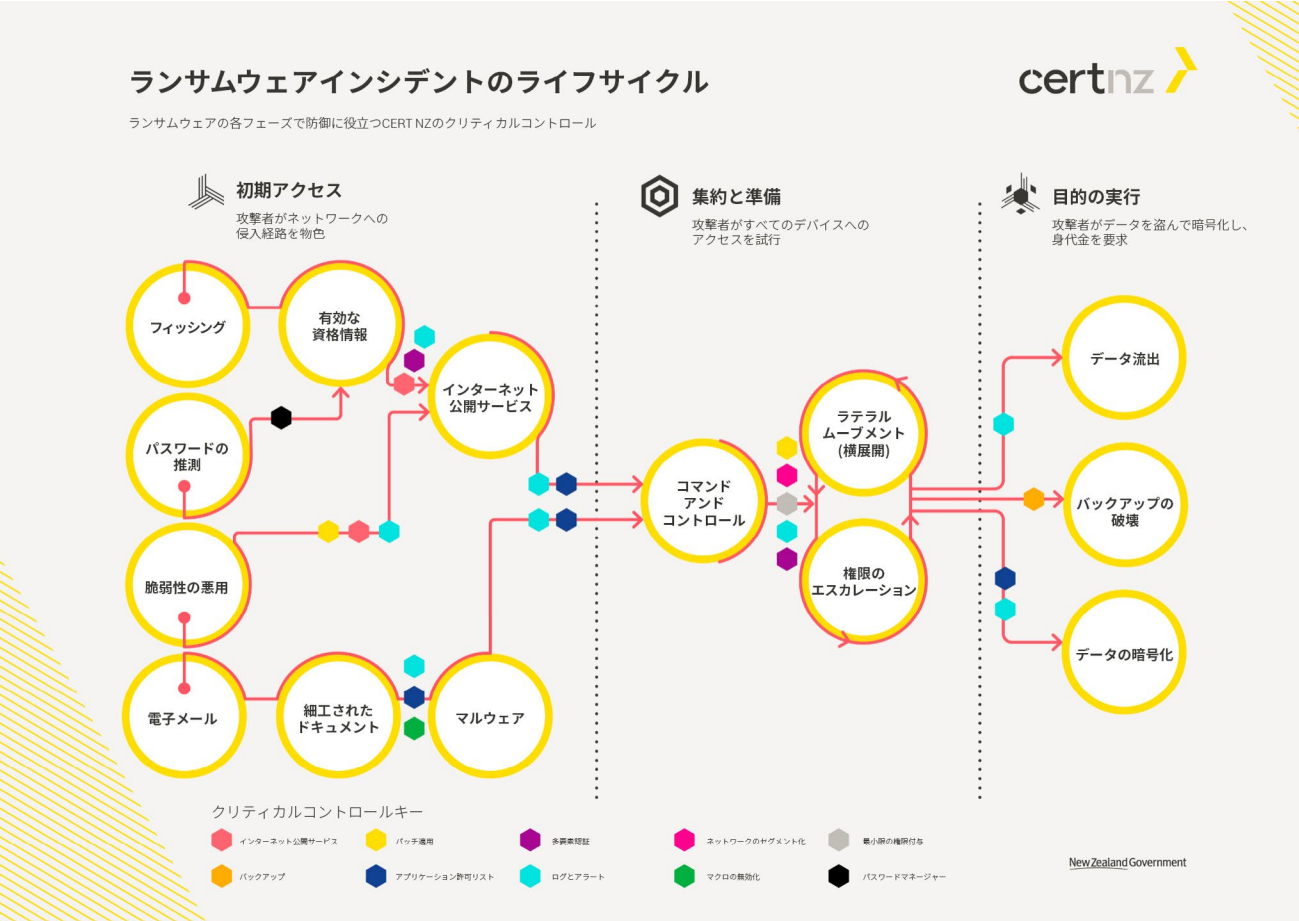

図2：CERT NZによるランサムウェアインシデントの詳細な推移

このCERT NZによる分析とMandiant社が突き止めた3日間という滞留時間は、ランサムウェアに先手を打つためのヒントを与えてくれます。しかし私たちは、防御策を検討する前に、次の2つの疑問について調べることにしました。

- ランサムウェアがホストを暗号化するのにかかる時間はどのくらいか？
- ファイルシステムの暗号化を完了するまでに、阻止したりファイルを復元したりすることができるか？

一部のランサムウェアが高速で暗号化できる理由は、リバースエンジニアリングによってかなり解明されています。しかし、さまざまなランサムウェアファミリーの暗号化速度を実験で比較した研究レポートは、LockBitランサムウェアグループによる宣伝以外に見つかりませんでした[6,7]。そこで私たちは、10種類のランサムウェアファミリーを対象に暗号化の速度を実験で検証しました。このホワイトペーパーでは、実験結果の分析と、ブルーチームが防御策を考える際に役立ついくつかの推奨事項をご紹介します。このホワイトペーパーの目的は、ランサムウェアの検出手法を確立することではない点に注意してください。目標は、セキュリティ関係者の皆様にランサムウェアの暗号化速度に関する包括的で正しい知識を紹介することです。

> Splunk SURGeは、10種類のランサムウェアファミリーを対象に暗号化の速度を実験で検証しました。このホワイトペーパーでは、実験結果の分析と、ブルーチームが防御策を考える際に役立つ推奨事項をご紹介します”

6. LockBitブログ、2022年2月13日参照、http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd[.]onion.ly/conditions
7. Gridinsoft社、「LockBit Ransomware.The Most Honest and the Fastest」、2022年1月29日参照、https://gridinsoft.com

前提

私たちはまずブレインストーミングを行い、ランサムウェアの暗号化速度はどのくらいか、それが予想以上に速かった場合に防御側はどの時点で対策すべきかなどの疑問から仮説を立てました[8]。そして最終的に、すべての疑問をまとめて、**攻撃者にひとたびシステムへのアクセスを許してランサムウェアをデプロイされてしまったら、現実的に阻止不可能な速さで暗号化が行われる**という仮説を立てました。Verizon社のDBIRによると、大半の組織では、侵害を検出するのは攻撃者がシステムへのアクセス権を獲得した数日後であり、数時間や数分後に検出できることはまれです[9]。私たちは上記の仮説を検証するために、テストを繰り返し行えるラボ環境を構築し、さまざまなランサムウェアバイナリのサンプルを収集して、結果を分析する必要がありました。また、調査はブルーチームの期待に応えられる方法で行いたいと考えました。そのため、ランサムウェアバイナリに対して静的なリバースエンジニアリングを行うのではなく、管理された環境下で実験を行い、同じ条件で各バイナリを測定することにしました。今回の調査の方法と技術的なプロセスの詳細は、今後、ブログ、レポート、カンファレンスで公開する予定です。

以下のセクションでは、仮説を検証するための実験の枠組みについて説明します。また、アーキテクチャの概要、マルウェアラボの構成、マルウェアの入手方法と選定理由についても説明します。さらに、調査と分析において結果のバイアスとなる可能性のある既知の想定も明示します。

調査方法

私たちの仮説を検証するには、管理された環境下で各種のランサムウェアを実行し、エンドポイントのホストからWindowsの機能を使ってパフォーマンステレメトリデータを収集して分析する必要があります。そこでまず、10種類のランサムウェアファミリーを選び、クラスター錯覚(実際はランダムなのにパターンに見えてしまう現象)と確証バイアス(自身の考えに沿った情報を無意識に集めてしまう傾向)を防ぐため、各ファミリーについて10個の異なるバイナリを用意することにしました。また、Windowsエンドポイントタイプとリソース仕様ごとに、各ファミリー用のアマゾン ウェブ サービス(AWS) VPC (Virtual Private Cloud)を1つ作成し、個々のバイナリをそれぞれの評価用に作成した専用ホストで実行します。結果は中央のSplunkインスタンスに転送し、そこで分析を行います。各ホストには、100個のディレクトリに9万8,561個のファイルを置きました。ファイルは、ランサムウェアバイナリが暗号化の標的にしがちなタイプのものを選び、Digital Corporaから入手しました[10,11,12]。これらのファイルはCC0ライセンスの下で提供され、元のファイルは米国政府のWebサイトで公開されています。最後に、ファイルの暗号化状況を把握し、各ランサムウェアファミリーの暗号化速度の測定基準とするために、WindowsホストでイベントID 4663を有効にしました[13]。

8. John McHale氏、「Defending DoD from Cyberattacks, Getting to the Left of the Boom - Military Embedded Systems」、2022年1月30日参照、http://militaryembedded.com/cyber/cybersecurity/defending-dod-from-cyberattacks-getting-to-the-left-of-the-boom
9. Verizon社、DBIR「2021 Data Breach Investigations Report」、90
10. Simson Garfinkel氏他、「Bringing Science to Digital Forensics with Standardized Forensic Corpora」、Digital Investigation 6 (2009年9月): S2–11、https://doi.org/10.1016/j.diin.2009.06.016
11. Digital Corpora Downloads: Corpora/Files/Govdocs1/By_type/、2022年1月30日参照、https://downloads.digitalcorpora.org/corpora/files/govdocs1/by_type/
12. Digital Corpora Downloads: Corpora/Files/Govdocs1/Zipfiles/、2022年1月30日参照、https://downloads.digitalcorpora.org/corpora/files/govdocs1/zipfiles/
13. Microsoft社、「4663(S) An Attempt Was Made to Access an Object」、((Windows 10) - Windows Security)、2022年1月30日参照、https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4663

ラボ環境

前述のとおり、この調査では、管理された環境下でランサムウェアバイナリを実行しました。Windowsの監査機能とログ機能を使ってランサムウェアのパフォーマンスデータを収集し、結果をSplunkインスタンスに転送します。テレメトリの設定は「実験手順」セクションで詳しく説明します。各ランサムウェアサンプルは、自己完結型の独立した環境内で実行しました。各ランサムウェア環境内のSplunkインスタンスから中央のSplunkインスタンスにイベントを転送し、そこで比較、分析、レポート作成を行います。ラボ環境の構築には、今回の実験用にカスタマイズしたオープンソースのSplunk Attack Rangeツールを使用しました(図3)[14]。Attack Rangeを使用すれば、TerraformとAnsibleを組み合わせてAWSを事前設定し、Splunkやログ機能を備えた小規模なネットワークを動的に作成できます。

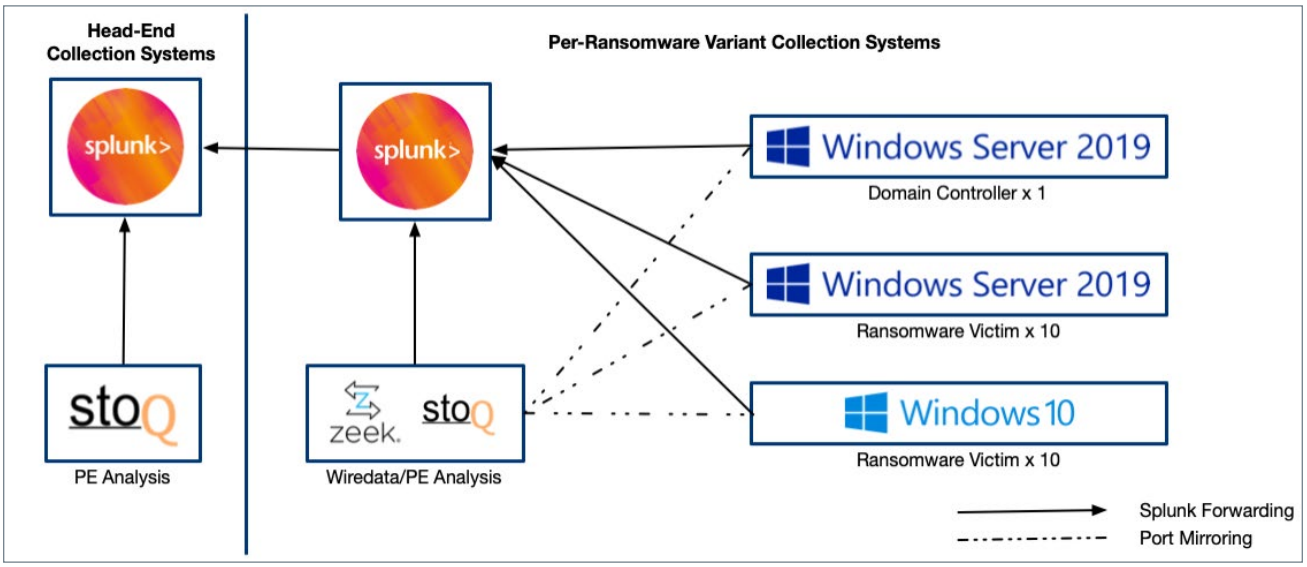

図3：カスタマイズしたAttack Rangeの概要

作成した領域内のホストは、参考に話を聞いた組織やPCMagなどの人気Webサイトの情報を基に、最新の一般的なラップトップやサーバービルドと同じ仕様に設定しました[15]。また、Microsoft Defenderをアンインストールし、ウイルス対策ツールやエンドポイント検出/対応(EDR)ツールは一切インストールしませんでした。そこに、Splunkに情報を転送するためのSplunkエージェントやMicrosoft Sysmonアプリケーションなどの追加ツールをインストールします[16]。最後に、ワーム(横展開)活動やリモート割り当てファイルの暗号化を検出できるように、ホストをWindowsドメインに参加させ、ドメインコントローラーでCドライブのネットワーク共有を有効にしました。ホストの仕様とログ設定の詳細は、付録AとBに記載しています。ファイル暗号化イベントを捕捉するために、テスト対象のディレクトリとすべてのサブディレクトリで、成功と失敗の両方のアクセス試行を記録するようにオブジェクトレベルの監査を有効にしました。オブジェクトレベルの監査を有効にすると、ランサムウェアバイナリがファイルを暗号化しようとするたびに、イベントコード4663のイベントが生成されます。ファイル暗号化の成功を示す最後の4663イベントはDELETE (削除アクセス権)であったため、これを暗号化速度の測定基準にしました。今回調査対象になったランサムウェアファミリーではすべてこのDELETEイベントが検出されましたが、他のファミリーでは検出されない可能性もあります。その場合は、TTEを測定するために別の基準を探す必要があります。

14. Splunk Attack Range、Jinja (2019年、転載：Splunk GitHub、2022年)、https://github.com/splunk/attack_range
15. PCMag、「Dell Latitude 7420 Review」、2022年1月30日参照、https://www.pcmag.com/reviews/dell-latitude-7420
16. markruss氏、Sysmon - Windows Sysinternals、2022年2月25日参照、https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

実験手順

最新のランサムウェア攻撃をできるだけ正確にエミュレートするために、調査では、Windows Server 2019ドメインコントローラー上に配置したリモートPowerShellスクリプトを使用して、10台のWindows 10ホストと10台のWindows Server 2019ホストでランサムウェアを実行しました。今回は、ユーザーが手動でバイナリを実行するのではなく、リモートPowerShellスクリプトを使用してランサムウェア感染を発生させる方法を採用しました。この方法には、デスクトップユーザーではなく運用担当者によってスクリプトを介して実行される最新のランサムウェア攻撃を再現できるメリットがあります。また、「人間の介入」のオーバーヘッドを減らすことにより、ランサムウェアにより多くのシステムリソースを使わせる狙いもあります。実行時にランサムウェアにはフラグを一切渡しませんでした。例外はBabukランサムウェアで、このランサムウェアはリモートPowerShellを使用する方法では実行の確実性が下がるため、各ホストで手動による実行を開始しました。ランサムウェアのパフォーマンスを評価するために、オペレーティングシステムごとに2つの異なるハードウェアプロファイルを割り当てました。これらのプロファイルの詳しい仕様は付録Bに記載しています。

PowerShellスクリプトでは、実行するランサムウェアサンプルを指定します。その後、ドメイン内のWindows 10またはWindows Server 2019ホストの数だけ実行を繰り返して、リモートWebサーバーからランサムウェアバイナリをダウンロードします。テストは常にWindows 10またはWindows Serverホストのいずれかで実行し、両方同時には行いません。

各ホストでダウンロードが完了したら、PowerShellスクリプトによって各ランサムウェアバイナリをリモートから実行します(Babukは除く)。その後、Windowsセキュリティイベントログに基づいて各バイナリがファイルを暗号化する速度を分析します。暗号化イベントを確実に捕捉するには、イベントコード4663 (オブジェクトへのアクセスが試行された)を確認する必要があります。必要なイベントログを生成するため、Windows 10とWindows Server 2019ホストにある100個のテスト用ディレクトリでファイルシステムの監査を有効にしました。

ランサムウェアバイナリ

10種類のランサムウェアファミリーの100個のランサムウェアサンプルは、VirusTotalから入手しました。ランサムウェアファミリーの分類は、VirusTotalでのMicrosoft Defenderの検出結果によってのみ判断しています。調査するランサムウェアファミリーは、過去12 ～ 24カ月で発生頻度が高かったものを選びました(図4)。

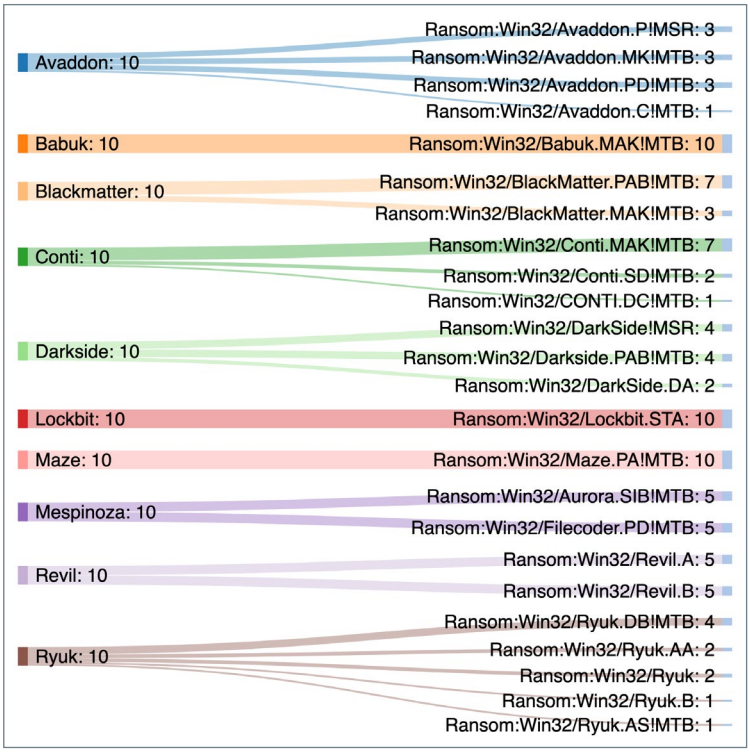

図4：調査対象になった10種類のランサムウェアファミリーとその亜種

各ファミリーで調査対象となった各バイナリのVirusTotal検出文字列とSHA256ハッシュは、付録Cに記載しています。

結果

ランサムウェアの暗号化速度は、ランサムウェアファミリーによって大きな差がありました。私たちは、サンプルごとの暗号化速度と時間とともに、ファミリー全体での暗号化速度の時間の中央値を調べました。平均値ではなく中央値を使用することにより、少数の外れ値を除外して、ファミリー全体の結果を公正に判断できます。

テスト中にWindows Perfmonデータを収集したところ、一部のファミリーは他に比べてシステムリソースの消費量が大きいことがわかりました。非常に効率的に動作するファミリーがある一方で、一部のファミリーはCPU時間を浪費し、ディスクアクセス率が大幅に上がる傾向があるようです。サンプル単位では、システムリソースの量と暗号化速度の間に直接的な相関関係は見られませんでした。 一部のランサムウェアファミリーは、高速なシステムでむしろパフォーマンスが落ちたり、クラッシュすることもありました。

サンプル別に見ると、9万8,561個のファイルの暗号化の最短時間は、4分9秒でした。この記録は、高レベル仕様のWindows Server 2019ホストで実行されたlockbit-9.exe (133adb408a4837d3a20634d79baf01151061c49cd936e9a8787b91df8997b6b0)によるものです(図5)。

Variant	Endpoint	process_name	Duration	Encryptions_Per_Second
Lockbit	Server-2019-High	C:\ransom\lockbit-9.exe	00:04:09	396

図5：Windows Server 2019ホストで実行されたlockbit-9.exeサンプルのデータ

逆に、同じテストファイルセットの暗号化の最長時間は、3時間35分8秒でした。この記録は、中レベル仕様のWindows 10ホストで実行されたbabuk-5.exe (1b9412ca5e9deb29aeaa37be05ae8d0a8a636c12fdff8c17032aa017f6075c02)によるものです(図6)。

Variant	Endpoint	process_name	Duration	Encryptions_Per_Second
Babuk	Win-10-Mid	C:\ransom\babuk-5.exe	03:35:08	8

図6：Windows 10ホストで実行されたbabuk-5.exeサンプルのデータ

各ファミリーの暗号化時間の中央値に注目すると、Babukには最長時間を記録したサンプルが1つ含まれるものの、ファミリー全体では2番目の速さで、中央値は6分34秒でした。全体の1位はやはりLockBitで、中央値は5分50秒です。ファミリー別で暗号化が最も遅かったのはMespinoza (PYSA)で、中央値は1時間54分54秒です。すべてのランサムウェアファミリーの暗号化時間の中央値は、42分52秒でした(図7)。

ファミリー	時間の中央値
LockBit	00:05:50
Babuk	00:06:34
Avaddon	00:13:15
Ryuk	00:14:30
Revil	00:24:16
BlackMatter	00:43:03
Darkside	00:44:52
Conti	00:59:34
Maze	01:54:33
Mespinoza (PYSA)	01:54:54
中央値の平均	**00:42:52**

図7：10種類のランサムウェアファミリーの暗号化時間の中央値

この中央値の時間の平均は、ランサムウェア攻撃で暗号化プロセスが始まってしまったら対応時間はあまり残されていないことを証明しています。最悪の想定として、侵害を受けたコンピューターの全データではなく、重要なファイル1つだけが暗号化の対象になるとしたら、時間はさらに限られます。この点を踏まえると、多くの組織にとって、暗号化プロセスの開始後にランサムウェア攻撃を緩和することは、不可能ではないとしても極めて困難だと言えるでしょう。この調査は、検出や防御策の確立までは目的としていませんが、ランサムウェア攻撃の対策を考える上で役に立つはずです。

私たちは、データの補足が、収集したデータの結果に影響しないように注意を払いました。実際には、Sysmonや制約のあるオブジェクトレベルの監査などのツールによる遅延を計測することは困難です。しかし、これらのツールが調査結果を大きく左右するほどの遅延を生じさせることはないと判断しました。ランサムウェアの暗号化速度に関する今後の調査では、ツールによる遅延を計測する手段を検討したいと考えています。もう1つ留意点として、ランサムウェアのサンプルをファミリーに分類するのは思ったよりも難しい作業でした。この調査では、サンプル選定の偏りをなくすために、VirusTotalで調べたMicrosoft Defenderの結果で各サンプルのハッシュを比較しました。そこからシグネチャ名を抽出し、正規化して、結果の値を基にランサムウェアファミリーを特定しました。

まとめと今後の展望

この調査の目的は、オペレーティングシステムやハードウェア仕様が異なるホストで主要なランサムウェアファミリーの暗号化速度を実験で測定することにより、組織が効果的な緩和策を講じるための時間が現実的にあるのかを検証することでした。中央値の結果によると、ランサムウェアの暗号化によって全データを喪失するまでの時間は43分以下です。データの暗号化と喪失はまさに、前述のサイバーキルチェーンで言う「目的実行」の段階です。M-Trendsレポートで明らかになった侵害検出までの平均時間が3日であることを考えると、43分の間に緩和策を講じるのは非常に厳しいでしょう。そのため私たちは、多くの組織にとってランサムウェアの暗号化からデータの喪失を防ぐことは実質的に不可能だと結論づけました。ランサムウェアからデータを保護するには、サイバーキルチェーンの「目的実行」段階ではなく、もっと前の「デリバリー」または「エクスプロイト」段階で手を打つ必要があります。この調査結果を、より効果的な緩和策の検討と実行にぜひお役立てください。なお、今回の調査では、ランサムウェアサンプルのワーム活動を検出できる環境を整備したものの、サンプルの中でこの活動をするものは少数でした。今後の調査では、ワーム活動についても詳しく調査したいと思います。

私たちの調査はこれで終わりではありません。まずは、Splunk BOSS Platformで今回の調査の全情報を公開して、この調査を裏付ける追加の調査を行う計画です。具体的には、ランサムウェアがファイルを暗号化するときの動作パターンの調査、ランサムウェアのワーム活動の検証、ファジーハッシュアルゴリズムに基づく類似ランサムウェアバイナリのクラスタリング、ランサムウェアファミリーの属性の経時的な分析を検討しています。

謝辞

今回のような調査は、主任調査担当者と副調査担当者だけでは成し得ません。ご協力いただいたAllie Mellen、Mark Harris、David French、Ryan Kovar、Audra Streetman、Marcus LaFerrera、Mick Baccio、Dave Herrald、Drew Church、Johan Bjerke、John Stoner、Tamara Chacon、Kelcie Bourne、Scott Roberts、Adam Swanda、Michael Haag (以上敬称略)、そしてSplunk脅威調査チーム(Splunk Threat Research Team：STRT)のSplunk Attack Range作成者の皆様に感謝申し上げます。

参考文献

- SDxCentral社、「Case Study: AIDS Trojan Ransomware」、2022年2月23日参照。
https://www.sdxcentral.com/security/definitions/case-study-aids-trojan-ransomware/
- PCMag、「Dell Latitude 7420 Review」、2022年1月30日参照。
https://www.pcmag.com/reviews/dell-latitude-7420
- Digital Corpora Downloads: Corpora/Files/Govdocs1/By_type/、2022年1月30日参照。
https://downloads.digitalcorpora.org/corpora/files/govdocs1/by_type/
- Digital Corpora Downloads: Corpora/Files/Govdocs1/Zipfiles/、2022年1月30日参照。
https://downloads.digitalcorpora.org/corpora/files/govdocs1/zipfiles/
- FireEye社/Mandiant社、Fireeye-Rpt-Mtrends-2021.Pdf、2021年4月13日。
https://www.mandiant.com/resources/m-trends-2021
- Simson Garfinkel氏、Paul Farrell氏、Vassil Roussev氏、George Dinolt氏、「Bringing Science to Digital Forensics with Standardized Forensic Corpora」、Digital Investigation 6 (2009年9月)：S2–11。
https://doi.org/10.1016/j.diin.2009.06.016
- CERT NZ、「How Ransomware Happens and How to Stop It」、2022年1月29日参照。
https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/
- Gridinsoft社、「LockBit Ransomware.The Most Honest and the Fastest.」、Gridinsoft社。2022年1月29日参照。
https://gridinsoft.com
- LockBitブログ、2022年2月13日参照。
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion[.]ly/conditions
- markruss氏、Sysmon - Windows Sysinternals、2022年2月25日参照。
https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
- John McHale氏、「Defending DoD from Cyberattacks, Getting to the Left of the Boom - Military Embedded Systems」、2022年1月30日参照。http://militaryembedded.com/cyber/cybersecurity/defending-dod-from-cyberattacks-getting-to-the-left-of-the-boom
- Microsoft社、「4663(S) An Attempt Was Made to Access an Object」((Windows 10) - Windows Security)、2022年1月30日参照。https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4663
- Microsoft Security Intelligence、「Trojan:PowerShell/Redearps.A」 Threat Description、2021年3月24日。https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:PowerShell/Redearps.A&threatId=-2147189091
- Splunk Attack Range、Jinja(2019年、転載：Splunk GitHub、2022年)。https://github.com/splunk/attack_range
- Symantec社、「THE INCREASED USE OF POWERSHELL IN ATTACKS」、Symantec Corporation、2016年。
https://docs.broadcom.com/doc/increased-use-of-powershell-in-attacks-16-en
- Verizon社、DBIR、「2021 Data Breach Investigations Report」、2021年5月12日。verizon.com/dbir

付録A：Windowsログ設定

- C:\Files\とすべてのサブディレクトリ(サブディレクトリ0 ～ 99)でWindowsファイルシステムの監査(イベントコード4633)を有効化(ファイル変更の失敗と成功の両方のログを有効化)
- コマンドラインからのWindowsプロセスの作成(イベントコード4688)のログを有効化
- Sysmonをインストールし、Olaf Hartong氏によるVerbose設定を適用

付録B：ホストの仕様

- Windows 10高レベル(Win-10-High)：Windows 10、AWS m5.2xlarge (8 CPU、32GB RAM)、300GB HDD (3000 IOPS、125MB/秒)
- Windows 10中レベル(Win-10-Mid)：Windows 10、AWS m5.xlarge (4 CPU、16GB RAM)、300GB HDD (3000 IOPS、125MB/秒)
- Windows Server 2019高レベル(Server-2019-High)：Windows Server 2019、AWS m5.4xlarge (16 CPU、64GB RAM)、300GB HDD (10000 IOPS、500MB/秒)
- Windows Server 2019中レベル(Server-2019-Mid)：Windows Server 2019、AWS m5.2xlarge (8 CPU、32GB RAM)、300GB HDD (3000 IOPS、125MB/秒)

付録C：ランサムウェアファミリーとバイナリ

バイナリ	SHA256ハッシュ	VirusTotalベンダー	VirusTotal検出
avaddon-0.exe	078de7d019f5f1e546aa29af7123643bd250341af71506e6256dfee8f245a2a7	Microsoft	Ransom:Win32/Avaddon.P!MSR
avaddon-1.exe	18c1ad49bf46b44df5926851ca30f00f6675c535b6826a3c779099643327ea33	Microsoft	Ransom:Win32/Avaddon.P!MSR
avaddon-2.exe	288165763637cda27304d90bb7ec47e103dfb69fdf6c009d113b1f6852c091a0	Microsoft	Ransom:Win32/Avaddon.MK!MTB
avaddon-3.exe	3a040105b3cb704c838a87061dba6b03712d308636a438004300ec154de2d4d6	Microsoft	Ransom:Win32/Avaddon.PD!MTB
avaddon-4.exe	4adc6cac6071cd67773c9cefab479f0ffde370c4cedac31b6db4de065c3ec7af	Microsoft	Ransom:Win32/Avaddon.PD!MTB
avaddon-5.exe	572610a5033a2060afa67ddbfd7345013e82c6904dd7ace22cb6f0b0bedcb550	Microsoft	Ransom:Win32/Avaddon.MK!MTB
avaddon-6.exe	743079700007b64647d9ea4a0c361e6e981518ed06a5902ab9f275c38aa45c7b	Microsoft	Ransom:Win32/Avaddon.MK!MTB
avaddon-7.exe	b9e62cb99e71c856cc41edfd837689993b7fc63c780e5786c34b2a8f63ef37b6	Microsoft	Ransom:Win32/Avaddon.P!MSR
avaddon-8.exe	cc95a8d100f70d0fbf4af14e852aa108bdb0e36db4054c3f60b3515818a71f46	Microsoft	Ransom:Win32/Avaddon.C!MTB
avaddon-9.exe	d8acd139f4f99b3137ab4cea9ef9e515e3a560f25a79666ac302f21d468340f8	Microsoft	Ransom:Win32/Avaddon.PD!MTB
babuk-0.exe	04126b30c1c2663cdf2b6386781aedbfce2ef418a0b01de510bd536903f577e3	Microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-1.exe	049e53f72c8afa5ccb850429d55a00e2fbe799e68247fd13f5058146cf0f4cf8	Microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-2.exe	106118444e0a7405c13531f8cd70191f36356581d58789dfc5df3da7ba0f9223	Microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-3.exe	12c561ac827c3f79afff026b0b1d3ddec7c4b591946e2b794a4d00c423b1c8f8	Microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-4.exe	1b04e1fbddfcdb16a3d103e50261937815668d92d4909a15352dd5e2615adbf4	Microsoft	Ransom:Win32/Babuk.MAK!MTB

バイナリ	SHA256ハッシュ	VirusTotal ベンダー	VirusTotal検出
babuk-5.exe	1b9412ca5e9deb29aeaa37be05ae8d0a8a636c12fdff8c17032aa017f6075c02	Microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-6.exe	1f37064ff61211d7a0d0428af856323bafb734b3f8b0e44d04e8e0db872349ee	Microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-7.exe	245e191bfe998ad9ef2d6b169af22f3c290e9950234f8ddd0f4a03cb3eebf761	Microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-8.exe	2509e5a4535d25110663a698410847aa0cb9ce734722076ada4c651532f318a5	Microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-9.exe	25835a890a218fd26bfd8b23696576402b5eb8a4c9af4a51529e14c4f00a9cce	Microsoft	Ransom:Win32/Babuk.MAK!MTB
blackmatter-0.exe	8eada5114fbbc73b7d648b38623fc206367c94c0e76cb3b395a33ea8859d2952	Microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-1.exe	26a7146fbed74a17e9f2f18145063de07cc103ce53c75c8d79bbc5560235c345	Microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-2.exe	2aad85dbd4c79bd21c6218892552d5c9fb216293a251559ba59d45d56a01437c	Microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-3.exe	496cd9b6b6b96d6e781ab011d1d02ac3fc3532c8bdd07cae5d43286da6e4838d	Microsoft	Ransom:Win32/BlackMatter.MAK!MTB
blackmatter-4.exe	b4b9fdf30c017af1a8a3375218e43073117690a71c3f00ac5f6361993471e5e7	Microsoft	Ransom:Win32/BlackMatter.MAK!MTB
blackmatter-5.exe	6d4712df42ad0982041ef0e2e109ab5718b43830f2966bd9207a7fac3af883db	Microsoft	Ransom:Win32/BlackMatter.MAK!MTB
blackmatter-6.exe	be5bc29f58b868f4ff8cd66b4526535593e515a697bb8951c625bdfed13cccb7	Microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-7.exe	ed47e6ecca056bba20f2b299b9df1022caf2f3e7af1f526c1fe3b8bf2d6e7404	Microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-8.exe	7a223a0aa0f88e84a68da6cde7f7f5c3bb2890049b0bf3269230d87d2b027296	Microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-9.exe	9bae897c19f237c22b6bdc024df27455e739be24bed07ef0d409f2df87eeda58	Microsoft	Ransom:Win32/BlackMatter.PAB!MTB
conti-0.exe	004ede55a972e10d9a21bcf338b4907d6eed65bf5ad6abbbd5aec7d8484bdedf	Microsoft	Ransom:Win32/Conti.SD!MTB
conti-1.exe	17ac91a36237d8f37dcee961ba74c9310a45c009780ea092c3a1e428870ff8a1	Microsoft	Ransom:Win32/Conti.MAK!MTB
conti-2.exe	34366c9a9ac34dd9016abd406cffe713a3e8606e8600e6cb07e0242904f91a5b	Microsoft	Ransom:Win32/Conti.MAK!MTB
conti-3.exe	49dc5a243d322cd4d467e5f24b61ff749869564ddcf6a2f700839cf5ae9e37ea	Microsoft	Ransom:Win32/Conti.MAK!MTB
conti-4.exe	0b0b902af452e1c949a609a3b29a9de21dac639846c77427de06e6e63c1fe904	Microsoft	Ransom:Win32/Conti.MAK!MTB
conti-5.exe	73bd8c2aa71f5dcd9d2ddd79e53656c6ae3db2535e08cf9dab1cd13bdd6d5ea3	Microsoft	Ransom:Win32/CONTI.DC!MTB
conti-6.exe	8df9b346bf591629a9eb0bf9f32c545a1266873495ceec9ba990be1dd22b9aa9	Microsoft	Ransom:Win32/Conti.MAK!MTB
conti-7.exe	0ffbc914e3bb09df586a93e5a5a557d03c5fcce7e8ee4a36bd3a09b8ed429c7a	Microsoft	Ransom:Win32/Conti.SD!MTB
conti-8.exe	d43b52e3453ce77d2694a239232f39341a98fa704954a558125e74a85f22a346	Microsoft	Ransom:Win32/Conti.MAK!MTB
conti-9.exe	1201e76d42f85feb89d64e6fd497144ed3afe66281b2464e84f3b889f2867c9b	Microsoft	Ransom:Win32/Conti.MAK!MTB
darkside-0.exe	22d7d67c3af10b1a37f277ebabe2d1eb4fd25afbd6437d4377400e148bcc08d6	Microsoft	Ransom:Win32/DarkSide!MSR

バイナリ	SHA256ハッシュ	VirusTotal ベンダー	VirusTotal検出
darkside-1.exe	2c323453e959257c7aa86dc180bb3aaaa5c5ec06fa4e72b632d9e4b817052009	Microsoft	Ransom:Win32/Darkside.PAB!MTB
darkside-2.exe	45ecce9dfec886e2b092a996f6affb9e7417d6121e58b0ec643be7e36a03106d	Microsoft	Ransom:Win32/Darkside.PAB!MTB
darkside-3.exe	7f6dd0ca03f04b64024e86a72a6d7cfab6abccc2173b85896fc4b431990a5984	Microsoft	Ransom:Win32/DarkSide!MSR
darkside-4.exe	84af3f15701d259f3729d83beb15ca738028432c261353d1f9242469d791714f	Microsoft	Ransom:Win32/Darkside.PAB!MTB
darkside-5.exe	c6e2ef30a86baa670590bd21acf5b91822117e0cbe6060060bc5fe0182dace99	Microsoft	Ransom:Win32/Darkside.PAB!MTB
darkside-6.exe	2c1e20a4b38634b97de398246bc3c8082d47663702a46bb885dc7fcc5f71daa1	Microsoft	Ransom:Win32/DarkSide!MSR
darkside-7.exe	43e61519be440115eeaa3738a0e4aa4bb3c8ac5f9bdfce1a896db17a374eb8aa	Microsoft	Ransom:Win32/DarkSide!MSR
darkside-8.exe	533672da9d276012ebab3ce9f4cd09a7f537f65c6e4b63d43f0c1697e2f5e48d	Microsoft	Ransom:Win32/DarkSide.DA
darkside-9.exe	5da3e6b4bea1eaceddb048a4a6bd702291189f42d15c4b2670de78984329b0a9	Microsoft	Ransom:Win32/DarkSide.DA
lockbit-0.exe	00ad914476509f84b40f2dbe804dc7c37a1a24ef3472674574d3367079bf0a2a	Microsoft	Ransom:Win32/Lockbit.STA
lockbit-1.exe	04f65270c92dda82c759c1eee49cf8f4c98a2ed0071272e49132331fda482dba	Microsoft	Ransom:Win32/Lockbit.STA
lockbit-2.exe	082f91d85c437f415cea44b36afb4198da07b78593c836a398cd96365166e7d8	Microsoft	Ransom:Win32/Lockbit.STA
lockbit-3.exe	50d08c974f7abce2da5c2a8976d3c6017334a418359d7bb031bd0914b848b24a	Microsoft	Ransom:Win32/Lockbit.STA
lockbit-4.exe	0cd33e6b180862072a00a0c2f897afa754df071bcec3d13e581c41a5c27a3102	Microsoft	Ransom:Win32/Lockbit.STA
lockbit-5.exe	7a1fb0eac9b62ce510030f9ff983d9d6225fd8dad6f05c1051c335aca87ffa24	Microsoft	Ransom:Win32/Lockbit.STA
lockbit-6.exe	0d4966b4724f141adb7a7db1d9ae48f5c293c6049cc7f949220256c2e72ab5ac	Microsoft	Ransom:Win32/Lockbit.STA
lockbit-7.exe	bb736c8d3dd2b3ebcacd3e2a61f95b20d23bc981cc22888dff88cfd2e720ee99	Microsoft	Ransom:Win32/Lockbit.STA
lockbit-8.exe	d68cad561a949648a84ffc2f2db186f585cd4a90951eea91c1c100d996cb3688	Microsoft	Ransom:Win32/Lockbit.STA
lockbit-9.exe	133adb408a4837d3a20634d79baf01151061c49cd936e9a8787b91df8997b6b0	Microsoft	Ransom:Win32/Lockbit.STA
maze-0.exe	f03172bd32ed16df6dda8e8146d24b073b864da59d669218fcc5e97835a5e956	Microsoft	Ransom:Win32/Maze.PA!MTB
maze-0.exe	f03172bd32ed16df6dda8e8146d24b073b864da59d669218fcc5e97835a5e956	Microsoft	Ransom:Win32/Maze.PA!MTB
maze-1.exe	0b9c99276ed36110afc58b3fb59ada135146180189c25d99618ca5897537ee21	Microsoft	Ransom:Win32/Maze.PA!MTB
maze-2.exe	2a6c602769ac15bd837f9ff390acc443d023ee62f76e1be8236dd2dd957eef3d	Microsoft	Ransom:Win32/Maze.PA!MTB
maze-3.exe	b3473d205ba722e229f49002093b61fc35902e1a67bcd558bf9a7811278e5cb2	Microsoft	Ransom:Win32/Maze.PA!MTB
maze-4.exe	5a06ae8540d5a0d7fb88e80d3e61c3a6079f3abdafe998ce70ffdcac9e940520	Microsoft	Ransom:Win32/Maze.PA!MTB
maze-5.exe	877c439da147bab8e2c32f03814e3973c22cbcd112d35bc2735b803ac9113da1	Microsoft	Ransom:Win32/Maze.PA!MTB

バイナリ	SHA256ハッシュ	VirusTotal ベンダー	VirusTotal検出
maze-6.exe	9d86beb9d4b07dec9db6a692362ac3fce2275065194a3bda739fe1d1f4d9afc7	Microsoft	Ransom:Win32/Maze.PA!MTB
maze-8.exe	e45eacf5158bb2aa11f29f0675b4cb68dbf7e376569516fe33f84be524c67763	Microsoft	Ransom:Win32/Maze.PA!MTB
maze-9.exe	ecd04ebbb3df053ce4efa2b73912fd4d086d1720f9b410235ee9c1e529ea52a2	Microsoft	Ransom:Win32/Maze.PA!MTB
mespinoza-0.exe	0433efd9ba06378eb6eae864c85aafc8b6de79ef6512345294e9e379cc054c3d	Microsoft	Ransom:Win32/Aurora.SIB!MTB
mespinoza-1.exe	0f0014669bc10a7d87472cafc05301c66516857607b920ddeb3039f4cb8f0a50	Microsoft	Ransom:Win32/Filecoder.PD!MTB
mespinoza-2.exe	164cb8e82d7e07cca0409925cadd8be5e3e8e07db88526ff7fe87596c6a6bd07	Microsoft	Ransom:Win32/Aurora.SIB!MTB
mespinoza-3.exe	4dc802894c45ec4d119d002a7569be6c99a9bba732d0057364da9350f9d3659b	Microsoft	Ransom:Win32/Aurora.SIB!MTB
mespinoza-4.exe	1e2009549452ed6b524b94ed683079ee60c2b9542b1bfd5b9ee42e9161d5e7c8	Microsoft	Ransom:Win32/Filecoder.PD!MTB
mespinoza-5.exe	327934c4c11ba37f42a91e1b7b956d5a4511f918e63047a8c4aa081fd39de6d9	Microsoft	Ransom:Win32/Aurora.SIB!MTB
mespinoza-6.exe	425945a93beb160f101d51de36363d1e7ebc45279987c3eaf5e7f183ed0a3776	Microsoft	Ransom:Win32/Filecoder.PD!MTB
mespinoza-7.exe	44f1def68aef34687bfacf3668e56873f9d603fc6741d5da1209cc55bdc6f1f9	Microsoft	Ransom:Win32/Aurora.SIB!MTB
mespinoza-8.exe	4770a0447ebc83a36e590da8d01ff4a418d58221c1f44d21f433aaf18fad5a99	Microsoft	Ransom:Win32/Filecoder.PD!MTB
mespinoza-9.exe	48355bd2a57d92e017bdada911a4b31aa7225c0b12231c9cbda6717616abaea3	Microsoft	Ransom:Win32/Filecoder.PD!MTB
revil-0.exe	d74cd044351030290f6ad8f70f91d51b6c39675ca3c70c45b5b0c5bd09589ff6	Microsoft	Ransom:Win32/Revil.A
revil-1.exe	338e8f24eeb38b5ef67ef662b65d592c816eba94dfaaac856021dac407daf294	Microsoft	Ransom:Win32/Revil.A
revil-2.exe	ab53e6823e47b446a245374c7760006ee84c8ea457a5fe9ca9df4732bf55a32a	Microsoft	Ransom:Win32/Revil.A
revil-3.exe	73dd3cb487dfb863304d9f6d79f60b2ab4adbd162e460a2210b4a6abf049ea53	Microsoft	Ransom:Win32/Revil.B
revil-4.exe	151271bf05310f94cd33cba3eb90be264edc4828c04e4e82f492b8e2576ee7a6	Microsoft	Ransom:Win32/Revil.B
revil-5.exe	97f905bb24c5054d09fe79a20e04fe84042ad985b5c6e09afad21efa83dcd7a0	Microsoft	Ransom:Win32/Revil.A
revil-6.exe	19f1a30555b83f23acc245ef6fe745f3292ef015c71abef8daa077e31f259179	Microsoft	Ransom:Win32/Revil.B
revil-7.exe	1f7b15f6cf07c5943ce8ab5bfd0700e4919808fca4260ffd2a509100d45fadaf	Microsoft	Ransom:Win32/Revil.B
revil-8.exe	1fb842e87f23e37ab39e201a024845c323c3d239331768db694dca96ed53d8c7	Microsoft	Ransom:Win32/Revil.B
revil-9.exe	21bcb9c0095424a179399379939f6ebdf1dfe202825c1ca5acdd25a8f751402f	Microsoft	Ransom:Win32/Revil.A
ryuk-0.exe	487d4698c6c938ca3e9251827a5813ddd21e26584b3459d768e457ddd4e8c4d4	Microsoft	Ransom:Win32/Ryuk.DB!MTB
ryuk-1.exe	4cb0bf61d61ad3383636df11b3e4da8e67bb0acea03e981ecdd48d08ed8c796c	Microsoft	Ransom:Win32/Ryuk.AA
ryuk-2.exe	dea1b54618643ffe59506398f0f131300abe0988da89b5414955843ae5b53fee	Microsoft	Ransom:Win32/Ryuk.DB!MTB

バイナリ	SHA256ハッシュ	VirusTotal ベンダー	VirusTotal検出
ryuk-3.exe	0cf36731f5b8651d53fc651607c3fccac24b631c08dca4493d8e07d2fbff1db3	Microsoft	Ransom:Win32/Ryuk.AA
ryuk-4.exe	8027a5e9dfcb379592868fb61fd8ed5f1605f0e4460db53d23a859d2a9743b91	Microsoft	Ransom:Win32/Ryuk.DB!MTB
ryuk-5.exe	d4b8cbfa94bac3dbd58452fcc6c4e0b56b65a54a671a2184d9fb6e3694a0266f	Microsoft	Ransom:Win32/Ryuk.DB!MTB
ryuk-6.exe	ba595e53ea6b0ef7f3332c2fec6a644c3cbc9756d2978c49e69eba92526904d8	Microsoft	Ransom:Win32/Ryuk.B
ryuk-7.exe	fc4d44faf906e7a6ba133dae5f33ce22b8569943574ffccadd0292b12abcc8fa	Microsoft	Ransom:Win32/Ryuk.AS!MTB
ryuk-8.exe	fe55650d8b1b78d5cdb4ad94c0d7ba7052351630be9e8c273cc135ad3fa81a75	Microsoft	Ransom:Win32/Ryuk
ryuk-9.exe	568d73074880063d4d2b3e9d3ddb938685de8ec8e24974ff32f5f47d55a2dcb0	Microsoft	Ransom:Win32/Ryuk

付録D：暗号化の対象になったファイルタイプ

拡張子	ファイル数	合計サイズ(MB)
html	25364	1,589.66
pdf	25185	15,116.11
txt	14856	12,632.61
doc	7955	5,019.95
jpg	7095	1,020.12
ppt	5576	11,044.64
xls	4238	4,384.81
gif	2010	114.83
ps	1186	2,024.57
csv	1005	224.24
xml	918	137.19
gz	794	435.43
log	514	622.12
unk	433	63.2
png	317	19.12
text	184	136.18
dbase3	170	3.03
f	129	14.11
rtf	128	31.35
eps	67	14.23
pps	65	164.05
swf	43	20.41
wp	42	4.2
fits	39	58.58
tex	36	2.25

拡張子	ファイル数	合計サイズ(MB)
java	36	1.24
kml	32	4.03
kmz	28	2
pptx	21	75.78
troff	21	1.9
bmp	13	5.23
docx	13	0.85
sgml	9	0.22
sql	7	0.46
hlp	7	0.02
dwf	5	0.56
gls	5	0.02
tmp	4	0.9
data	2	0.77
拡張子なし	1	124.94
zip	1	0.84
vrml	1	0.32
wk1	1	0.31
py	1	0.23
ttf	1	0.12
g3	1	0.12
xlsx	1	0.05
pub	1	0.000049
	計98,561個	**計53.83 GB**

付録E：エンドポイント別のパフォーマンス集計

Windows Server 2019高レベル仕様

Endpoint Specifications

Endpoint	OS	CPU Cores	GB RAM	Disk IOPS	Disk Throughput MB/s
Win-10-Mid	Windows 10	4	16	3000	125
Win-10-High	Windows 10	8	32	3000	125
Server-2019-Mid	Windows Server 2019	8	32	3000	125
Server-2019-High	Windows Server 2019	16	64	10000	500

Median Resource Utilization

Variant	Endpoint	%_Privileged_Time	%_Processor_Time	%_User_Time	Handle_Count	Thread_Count	Priority	Page_Faults/sec	IO_Read_KBytes/sec	IO_Write_KBytes/sec	Private_MBytes	Virtual_MBytes	Working_Set(MBytes)
Avaddon	Server-2019-High	95.52	96.18	61.64	628.67	67.62	8	167890.42	54246.70	55118.46	17.28	227.62	26.13
Babuk	Server-2019-High	34.82	99.74	99.36	452.19	67.89	8	3853.88	28099.74	26860.70	25.72	178.65	19.27
Blackmatter	Server-2019-High	8.25	11.90	5.47	313.81	35.74	10	1962.33	10263.18	10283.99	12.70	117.03	16.99
Conti	Server-2019-High	6.88	12.97	8.59	257.58	18.58	8	343.72	11532.70	11492.30	164.83	237.50	17.46
Darkside	Server-2019-High	6.94	21.29	16.21	311.21	35.54	10	1670.40	8721.45	8731.53	12.00	113.81	16.41
Lockbit	Server-2019-High	27.02	41.55	15.94	502.12	28.07	8	1531.18	1237.26	1399.21	7.79	110.66	19.06
Maze	Server-2019-High	4.29	5.88	4.40	365.64	3.38	8	2086.59	13216.13	4831.49	4.19	86.45	16.28
Mespinoza	Server-2019-High	5.76	7.54	4.97	153.03	2.03	8	64.42	8191.90	6142.31	3.48	47.67	8.07
Revil	Server-2019-High	7.06	18.38	13.29	243.36	35.16	8	2425.00	14108.76	14068.99	11.61	105.26	15.01
Ryuk	Server-2019-High	53.31	86.33	20.02	171279.74	53.82	8	2931.32	62045.03	82201.84	181.45	296.14	102.16

Median Encryption Speeds

Variant	Endpoint	Total_Encryptions	Duration_In_Minutes	Encryptions_Per_Minute	Encryption_Speed_MB_Per_Second
Avaddon	Server-2019-High	43868	7.58	5787.00	53.9
Babuk	Server-2019-High	98560	5.55	17760.00	166
Blackmatter	Server-2019-High	98553	37.41	2635	24.55
Conti	Server-2019-High	98560	64.07	1538	14.34
Darkside	Server-2019-High	98553	43.60	2260	21.07
Lockbit	Server-2019-High	98548	5.30	18622	173
Maze	Server-2019-High	98560	86.53	1139	10.62
Mespinoza	Server-2019-High	97080	102.55	946.70	8.824
Revil	Server-2019-High	98553	27.25	3618	33.71
Ryuk	Server-2019-High	89521	8.92	9266	93.6

Windows Server 2019中レベル仕様

Endpoint Specifications

Endpoint	OS	CPU Cores	GB RAM	Disk IOPS	Disk Throughput MB/s
Win-10-Mid	Windows 10	4	16	3000	125
Win-10-High	Windows 10	8	32	3000	125
Server-2019-Mid	Windows Server 2019	8	32	3000	125
Server-2019-High	Windows Server 2019	16	64	10000	500

Median Resource Utilization

Variant	Endpoint	%_Privileged_Time	%_Processor_Time	%_User_Time	Handle_Count	Thread_Count	Priority	Page_Faults/sec	IO_Read_KBytes/sec	IO_Write_KBytes/sec	Private_MBytes	Virtual_MBytes	Working_Set(MBytes)
Avaddon	Server-2019-Mid	95.42	97.16	51.46	467.96	35.69	8	166866.12	44362.49	45706.62	14.84	140.11	23.97
Babuk	Server-2019-Mid	29.07	160.58	147.78	380.75	36.21	8	2985.14	21796.16	20907.03	17.95	133.61	16.87
Blackmatter	Server-2019-Mid	7.40	9.33	4.55	313.49	19.62	10	1688.89	8863.80	8850.98	11.45	95.38	16.49
Conti	Server-2019-Mid	7.10	12.33	7.93	241.00	10.41	8	117.35	10851.88	10881.95	83.15	145.91	16.57
Darkside	Server-2019-Mid	6.23	18.67	14.12	332.28	19.48	10	1495.22	7732.50	7725.44	10.86	95.34	16.22
Lockbit	Server-2019-Mid	22.40	33.26	13.45	458.79	18.10	8	1205.07	975.23	1092.23	7.02	96.55	18.76
Maze	Server-2019-Mid	4.02	4.94	3.95	333.54	4.46	8	1572.07	10751.79	3887.37	3.46	68.76	13.73
Mespinoza	Server-2019-Mid	5.39	6.70	4.65	153.03	2.02	8	80.30	6782.18	5023.70	3.55	47.27	8.11
Revil	Server-2019-Mid	6.62	17.54	12.86	254.25	19.30	8	2147.04	12687.87	12605.01	11.11	86.37	15.27
Ryuk	Server-2019-Mid	41.19	59.49	14.45	218856.14	53.61	8	1965.13	38545.07	56935.97	182.73	300.70	102.88

Median Encryption Speeds

Variant	Endpoint	Total_Encryptions	Duration_In_Minutes	Encryptions_Per_Minute	Encryption_Speed_MB_Per_Second
Avaddon	Server-2019-Mid	50307	8.75	5749.00	53.6
Babuk	Server-2019-Mid	98560	6.51	15140.00	141
Blackmatter	Server-2019-Mid	98553	43.18	2283	21.27
Conti	Server-2019-Mid	98560	67.60	1458	13.59
Darkside	Server-2019-Mid	98553	50.47	1953	18.20
Lockbit	Server-2019-Mid	98548	6.76	14594	136
Maze	Server-2019-Mid	98560	114.75	858.94	8.006
Mespinoza	Server-2019-Mid	97080	124.55	779.48	7.265
Revil	Server-2019-Mid	98553	29.56	3336	31.07
Ryuk	Server-2019-Mid	93014	12.67	7289	68.4

Windows 10高レベル仕様

Endpoint Specifications

Endpoint	OS	CPU Cores	GB RAM	Disk IOPS	Disk Throughput MB/s
Win-10-Mid	Windows 10	4	16	3000	125
Win-10-High	Windows 10	8	32	3000	125
Server-2019-Mid	Windows Server 2019	8	32	3000	125
Server-2019-High	Windows Server 2019	16	64	10000	500

Median Resource Utilization

Variant	Endpoint	%_Privileged_Time	%_Processor_Time	%_User_Time	Handle_Count	Thread_Count	Priority	Page_Faults/sec	IO_Read_KBytes/sec	IO_Write_KBytes/sec	Private_MBytes	Virtual_MBytes	Working_Set(MBytes)
Avaddon	Win-10-High	68.96	77.37	31.62	457.12	37.10	8	88500.41	28297.32	28647.71	15.05	168.35	23.63
Babuk	Win-10-High	38.54	94.00	93.48	376.90	37.86	8	3189.90	21838.42	21783.18	19.83	151.92	17.53
Blackmatter	Win-10-High	6.74	8.91	4.58	299.34	21.56	10	1598.82	8358.30	8351.87	10.45	108.34	15.39
Conti	Win-10-High	7.95	15.24	9.83	228.03	11.32	8	261.15	12402.19	12389.49	83.23	167.86	15.25
Darkside	Win-10-High	6.90	20.24	15.05	393.16	23.78	10	1665.17	8488.67	8470.35	10.75	114.21	17.02
Lockbit	Win-10-High	28.78	44.13	17.42	498.25	24.38	8	1440.13	1251.17	1417.23	9.20	119.75	20.38
Maze	Win-10-High	4.10	5.00	3.91	323.62	5.11	8	1564.34	10369.55	3806.94	3.70	85.59	14.08
Mespinoza	Win-10-High	6.23	7.29	4.68	144.07	2.24	8	147.27	7219.82	5397.70	3.58	61.30	8.30
Revil	Win-10-High	8.09	21.70	15.75	252.97	19.27	8	2732.09	17054.07	16986.81	10.48	100.22	14.25
Ryuk	Win-10-High	43.93	56.51	11.68	106061.45	64.46	8	1941.94	33521.11	41399.72	182.68	326.10	103.71

Median Encryption Speeds

Variant	Endpoint	Total_Encryptions	Duration_In_Minutes	Encryptions_Per_Minute	Encryption_Speed_MB_Per_Second
Avaddon	Win-10-High	98560	14.10	6990.00	65.2
Babuk	Win-10-High	98560	6.52	15130.00	141
Blackmatter	Win-10-High	98553	45.23	2179	20.31
Conti	Win-10-High	98560	58.30	1691	15.76
Darkside	Win-10-High	98553	45.38	2172	20.24
Lockbit	Win-10-High	98548	5.40	18259	170
Maze	Win-10-High	98560	115.45	853.71	7.957
Mespinoza	Win-10-High	97080	115.60	839.83	7.828
Revil	Win-10-High	98553	23.70	4160	38.76
Ryuk	Win-10-High	98284	17.17	5740	53.37

Windows 10中レベル仕様

Endpoint Specifications

Endpoint	OS	CPU Cores	GB RAM	Disk IOPS	Disk Throughput MB/s
Win-10-Mid	Windows 10	4	16	3000	125
Win-10-High	Windows 10	8	32	3000	125
Server-2019-Mid	Windows Server 2019	8	32	3000	125
Server-2019-High	Windows Server 2019	16	64	10000	500

Median Resource Utilization

Variant	Endpoint	%_Privileged_Time	%_Processor_Time	%_User_Time	Handle_Count	Thread_Count	Priority	Page_Faults/sec	IO_Read_KBytes/sec	IO_Write_KBytes/sec	Private_MBytes	Virtual_MBytes	Working_Set(MBytes)
Avaddon	Win-10-Mid	84.53	88.58	35.93	376.26	21.10	8	109298.88	31681.35	31810.25	8.82	145.11	18.33
Babuk	Win-10-Mid	28.88	92.38	91.30	342.77	21.67	8	2573.52	18024.88	17406.98	14.48	124.84	15.87
Blackmatter	Win-10-Mid	7.09	9.93	5.65	299.84	14.13	10	1713.94	9098.79	9079.02	9.82	98.72	14.88
Conti	Win-10-Mid	8.03	15.45	9.92	219.44	7.29	8	67.98	12578.51	12631.15	42.55	122.58	14.83
Darkside	Win-10-Mid	7.05	21.41	15.69	393.82	15.86	10	1647.89	8560.02	8550.47	10.30	104.35	16.85
Lockbit	Win-10-Mid	28.65	42.79	15.75	533.11	16.01	8	1319.68	1149.89	1246.13	10.74	111.46	20.72
Maze	Win-10-Mid	4.29	5.31	4.06	318.91	5.09	8	1561.72	10573.49	3707.72	3.63	82.95	13.79
Mespinoza	Win-10-Mid	6.39	7.56	4.79	144.08	2.23	8	137.56	7402.86	5527.32	3.58	61.26	8.23
Revil	Win-10-Mid	8.44	22.78	15.96	253.35	12.48	8	2710.56	16585.00	16521.51	9.70	91.44	14.05
Ryuk	Win-10-Mid	43.86	54.72	12.19	126006.82	63.22	8	1599.03	33496.12	41261.27	182.21	322.15	95.17

Median Encryption Speeds

Variant	Endpoint	Total_Encryptions	Duration_In_Minutes	Encryptions_Per_Minute	Encryption_Speed_MB_Per_Second
Avaddon	Win-10-Mid	98560	12.63	7804.00	72.7
Babuk	Win-10-Mid	98560	7.84	12580.50	117
Blackmatter	Win-10-Mid	98553	42.92	2297	21.40
Conti	Win-10-Mid	98560	59.34	1661	15.48
Darkside	Win-10-Mid	98553	44.72	2204	20.54
Lockbit	Win-10-Mid	98548	5.84	16881	157
Maze	Win-10-Mid	98560	115.12	856.19	7.980
Mespinoza	Win-10-Mid	97080	114.20	850.09	7.924
Revil	Win-10-Mid	98553	23.67	4166	38.81
Ryuk	Win-10-Mid	87739	16.98	5270	48.15

SURGeについて

2021年10月に創設されたSURGeは、世界的に影響をおよぼすサイバー脅威に関する調査、対応、教育を専門的に行う戦略的サイバーセキュリティ調査部門です。SURGeは、信頼できるアドバイザーとして、対応ガイドや詳細な分析を調査報告書、会議論文、またはウェビナーとして提供し、注目度が高く一刻を争うようなサイバー攻撃に直面した際に役立つ技術的なアドバイスを提供しています。組織はSURGeを利用して適切なコンテキスト情報や推奨事項をタイムリーに受け取ることができるため、グローバルなセキュリティインシデントにも確かな情報に基づいて対応することができます。詳細についてはこちらをご覧ください。

splunk>

営業へのお問い合わせはこちら：https://www.splunk.com/ja_jp/talk-to-sales.html

〒100-0004 千代田区大手町1-1-1 大手町パークビルディング 8階

www.splunk.com/ja_jp

splunkjp@splunk.com

22-23023-Splunk-EmpiricallyComparativeAnalysisofRansomwareBinaries-A4-WP-JA-202204