アンラボ・セキュリティレター

Press Ahn

2022.11　Vol.107

ランサムウェア組織に関する過去 2 年間の動向

ランサムウェア組織に関する過去 2 年間の動向

突然だが、あなたはランサムウェア攻撃を受けたことがあるだろうか？

今の時代、この質問に対し「受けたことがある」と回答する企業はそう少なくないだろう。ランサムウェアによる発生被害は、今年も留まるところを知らない。今も世界中で、複数のランサムウェア組織が様々なランサムウェアを用い、活発な活動を繰り広げているのが現状だ。

我々が一度は耳にしたことのあるランサムウェア組織は、一体どのように活動しているのか？また、彼らが使用するランサムウェアはどのように変化してきたのか？今回は、過去 2年間における主なランサムウェア組織、およびランサムウェアに関する動向を紹介していく。

ランサムウェア主要動向

1. ランサムウェア組織の特徴

まず、多くのランサムウェア組織は、サービス型ランサムウェア（Ransomware-as-a-Service：RaaS）という運営形態をなす。協力者を募り、収益を 2：8 または 1：9 で分配するなど、その姿は徐々に企業化してきている。

さらに、メディアや世間の関心、また捜査機関の調査によって、一部ランサムウェア組織のメンバーの検挙が相次いでいる。これに危機感を覚えたランサムウェア組織は、解散やリブランディング（再構築）を行っている。一例として、DarkSide（ダークサイド）ランサムウェア組織は、2021年 5月、米コロニアル・パイプライン（Colonial Pipeline）を標的としたランサムウェア攻撃後、捜査機関による監視が強まったことにより、組織を閉鎖し、名称を Black Matter（ブラックマター）に変え再び現れた。

問題は、これまで捜査機関に検挙されたメンバーのほとんどが、資金洗浄や流布を担当する者で、ランサムウェア組織の中心的な開発メンバーの大多数は、未だ検挙に至っていないという点だ。さらに、以前より活動していたランサムウェアグループが解散すると、構成メンバーらは別のランサムウェア組織に入社（？）することもある。

サイバー犯罪組織以外にも、国家支援を受けるとされる脅威グループがランサムウェアを使用する場合もある。以前、背後に北朝鮮の支援を受けているとされる Andariel（アンダリエル）グループが、韓国内でランサムウェア攻撃を敢行したことがある。米政府によると、北朝鮮の支援を受ける組織が、マウイランサムウェアを用い医療施設を攻撃したことが明らかになった。セキュリティ企業である Kaspersky（カスペルスキー）は、マウイランサムウェアと Andariel（アンダリエル）グループの関連性について公開している。

また、特定の地域でのみ活動するランサムウェア組織も存在する。韓国内でのみ活動するグループとして、Gwisin・Magniber・Masscan などが確認されている。

一部の攻撃者らは、ランサムウェア攻撃を敢行する際、情報流出を狙った InfoStealer（インフォスティーラー）も合わせて感染させることがある。暗号化したデータをもとに脅迫するだけに留まらず、感染者情報の流出による収益の最大化を狙っての動きとみられる。

2. ランサムウェア攻撃手法の進化

ランサムウェアの攻撃手法もまた進化し続けている。メール内に不正リンクやファイルを添付する方法以外にも、メールおよび Web サーバーの脆弱性を狙い侵入するケースもある。サプライチェーン（Supply Chain）を利用した内部侵入も知られているが、あまり一般的な方法ではない。一部のランサムウェアは、自己拡散機能も有している。

特定の対象を狙った標的型攻撃は、一般的なハッキングや APT（Advanced Persistent Threat）攻撃に類似している。初期侵入後、内部システムを 1つずつ掌握し、内部情報を流出させる攻撃過程は同じだが、最後にランサムウェアを流布するという点に違いがある。さらに、防御側はランサムウェア対策に向け様々なセキュリティ製品を使用しているが、これらを無効化、もしくは迂回するために多くの試みが行われている。

ランサムウェアの手法自体が進化を重ねる中、主な特徴として挙げられるのは次の 3つである。

1つ目は、クラウド環境の拡大に伴い、攻撃者も変化する環境に合わせ順応しているという点だ。Windows 用のランサムウェアだけでなく、クラウド環境を狙った Linux 用のランサムウェア製作も行われている。

2つ目に、従来のランサムウェアといえば、実行直後にファイルを暗号化し、ランサムノートを表示する手法をとっていた。しかし、Gwisin・Hive・LockBit などの近年のランサムウェアは、実行する上で引数値を必要とする。引数値がわからない場合、不正機能は実行されない。これにより、行為ベースのセキュリティ製品による検知を通過できるため、アナリストらもランサムウェアの有無を判断するのが困難となる。

3つ目に、Windows を対象とするランサムウェアの場合、ファイル暗号化の妨げになる正常サービスを終了させ、vssadmin.exe などを用いたボリュームシャドウ（Volume Shadow）コピーの削除、またはバックアップシステムの把握を行う。これにより、バックアップデータの復旧も難しくなる。

3. ランサムウェアの主な攻撃対象および事例

ここ 1年間に公開された分析レポートやアンラボの情報などをもとに、総合的な結果をまとめたものが、[表1] の ランサムウェア攻撃事例（2021~2022）である。

日付	国家	産業	内容
2021年 4月	イギリス	鉄道	マージーレール社（英国鉄道ネットワーク）が

			LockBit ランサムウェアに感染
2021年 8月	アメリカ	医療	米オハイオ州 Memorial Health System 社が Hive ランサムウェアに感染
2021年 8月	タイ	航空	LockBit ランサムウェアの感染により バンコクエアの顧客情報が流出
2021年 11月	韓国	食品	Hive ランサムウェアに感染
2022年 1月	フランス	法務部	LockBit ランサムウェアに感染
2022年 1月	-	製造	電力部品供給業者が、Conti ランサムウェアに感染
2022年 2月	韓国	重工業	Hive ランサムウェアに感染
2022年 4月	韓国	医療	Gwisin ランサムウェアのLinux 版を確認
2022年 5月	韓国	医療	Gwisin ランサムウェアに感染
2022年 5月	コスタリカ	政府	Conti ランサムウェア感染により コスタリカ政府が緊急事態宣言を発動
2022年 7月	韓国	IT	Masscan ランサムウェアに感染
2022年 7月	韓国	エネルギー	Masscan ランサムウェアに感染
2022年 7月	韓国	医療	Gwisin ランサムウェアに感染
2022年 7月	韓国	IT	LockBit 3.0 に感染
2022年 7月	韓国	製造	BlueCrab ランサムウェアに感染
2022年 7月	韓国	繊維製造	BitLocker を悪用したファイルの暗号化
2022年 7月	韓国	重工業	Hive ランサムウェアに感染
2022年 7月	韓国	医療	Masscan ランサムウェアに感染
2022年 8月	韓国	企業	BitLocker を悪用したファイルの暗号化

[表1] ランサムウェア攻撃事例 (2021~2022年)

韓国では、Hive・LockBit・Magniber などのランサムウェア攻撃が盛んに行われている。また、Gwisin・Masscan のように、韓国企業のみを狙ったランサムウェアの活動報告も後を絶たない。

4. 攻撃手法 (Attack Vectors)

ランサムウェア組織が用いる攻撃展開手法に関しては、一般的な攻撃者が用いる方法と比べ大きな差はない。

個人を対象にした攻撃の場合、主にメールや Web サイトをハッキング後、訪問ユーザーのシステムを感染させる手法を使用する。

しかし、攻撃対象が企業の場合、様々な方法が用いられる。Clop ランサムウェアの捜査内容によると、攻撃者は標的企業の職員700名にマルウェアが仕込まれたメールを送信し、そのうち 3名が添付ファイルを開いたことでマルウェアに感染、その後 52時間以内にランサムウェアが組織へと拡散された。

さらに、企業内で使用するデータベース・メール・Web サーバーの脆弱性を利用し侵入後、追加で内部システムを掌握することで、ファイルの配布機能をもつ資産管理プログラムなどから、ランサムウェアを流布するケースもある。

被害事例を見てみると、標的企業らはアクティブディレクトリ（Active Directory：AD）を運営する場合が多く、被害に遭ったシステムは、ローカルアドミン（Administrator、管理者）のアカウントが有効化されており、リモートデスクトップ接続（Remote Desktop Protocol：RDP）が可能な状態であった。AD サーバーのドメインコントローラでグループポリシーを作成し、現在のドメインに接続した別のパソコンへと、ランサムウェアファイルを配布する流れをとっている。

また、組織内で運営しているサーバーや職員への支給機器は、管理上の利便性のため、同一のパスワードを使用する場合が多い。そのため、予想以上に簡単に内部システムへと侵入されてしまう。

主なランサムウェアおよび組織の活動動向

[表2] の内容は、2022年に確認された主なランサムウェア組織の活動動向だ。続いて、近年盛んな活動を見せている 6つのランサムウェア組織に関する内容を紹介する。

組織名	ランサムウェア	活動状況	説明
BlackCat (ALPHV)	BlackCat	高	DarkSide・BlackMatter の後継と推測
REvil	BlueCrab (Sodinokibi)	並	GandCrab の後継
BlueSky	BlueSky	並	-
Clop	Clop	並	-
Wizard Spider	Conti	解散	内部情報の流出後、活動停止状態
Globeimposter	Globeimposter	並	-
Gwisin	Gwisin	並	韓国内でのみ活動
Hive	Hive	高	-
LockBit	LockBit	高	-
Magniber	Magniber	高	韓国内でのみ活発に活動
Masscan	Masscan	高	韓国内でのみ活動
Yanluowang	Yanluowang	並	-

[表2] 主なランサムウェア組織の活動動向

1. BitLocker を悪用した攻撃

攻撃時に、ランサムウェアではなく、Windows に標準搭載されている BitLocker が用いられる場合もある。BitLocker とは、▲Windows Server 2008、▲Windows 7、▲Vista 8・8.1・10・11 に内蔵されているディスクの暗号化機能だ。GUI（Gra

phic User Interface) や CLI (Command-Line Interface) でサポートされており、CLI 方式の場合、リモート操作での暗号化が可能なため、攻撃者に悪用されるケースもある。

リモート操作で BitLocker を実行するためには、対象システム内にて BitLocker サービスのスタートアップ設定が、”手動 (Windows のデフォルト設定)” 状態でなくてはならない。また、サービスの準備状態が ”自動” であったとしても、該当システムの管理者権限さえあれば実行することが可能だ。

BitLocker を悪用し、リモート操作で対象システムのドライブを暗号化する場合、コマンドを受けた対象システムは、該当ドライブの暗号化実行画面が表示された状態で暗号化が行われるため、被害側はリモート操作による暗号化を認識できる。しかし、 "-lock" 引数値を使用することで、暗号化の完了前にドライブへのアクセスを遮断することが可能だ。

主な攻撃動向を見てみると、2022年 8月、20社余りの韓国企業に対し、FRP (Fast Reverse Proxy) を利用した攻撃が続けて確認されている。攻撃事例としては、まず脆弱性のあるサーバーに侵入後、Web シェルをインストールすることで、Reverse Shell 設定および RDP への接続を行い、最後に BitLocker を有効化し、C ドライブを除く全てのドライブを暗号化していた。

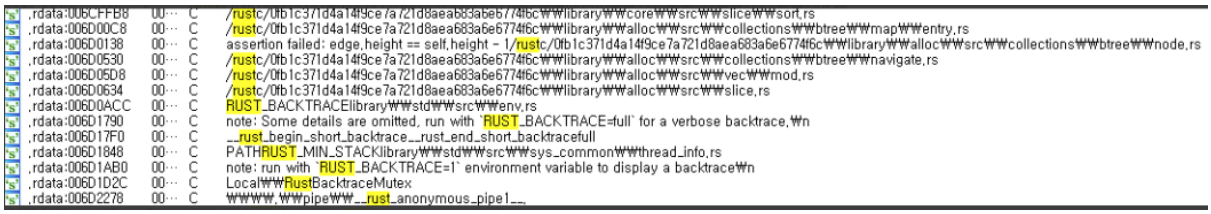
Lorenz ランサムウェア組織の場合、Mitel 社製の VoIP 機器 (MiVoice) における 脆弱性 (CVE-2022-29499) を利用し侵入後、Lorenz ランサムウェアおよび BitLocker を用いて攻撃を敢行している。

BitLocker のリモート実行を予防するためには、BitLocker 機能を使用しない場合、必ずサービス中断状態にし、サービスのスタートアップ設定を “無効” にしておく必要がある。

2. BlackCat (ALPHV)

BlackCat は、 別名 ALPHV、Noberus などと呼ばれ、Rust 言語で開発されたランサムウェアである。2021年 12月、ダークウェブ上のフォーラムで公開されたが、実際の活動は 2021年 11月末から確認されている。被害企業の所属国家を見てみると、アメリカが最も多く、次いでカナダ、オーストラリア、イギリスの順となっている。

BlackCat ランサムウェアは、RaaS (Ransomware as a Service、サービスとしてのランサムウェア) 形態のビジネスモデルで運営されている。製作者は、攻撃者 (系列会社) を募り、収益の 10～20% を開発者、残りの利益を攻撃者に分配していることで知られている。Windows および Linux 版があり、Rust 言語でコンパイルする特徴を持つ。関連する文字列は [図1] のとおりだ。



[図1] BlackCat ランサムウェアの特徴的な文字列

3. Gwisin

Gwisin は、2021年 9月から韓国企業だけを狙い攻撃を敢行しているランサムウェア組織である。組織名 (Gwisin / 귀신 / クィシン：お化け、幽霊、ゴーストの意) からもわかるように、韓国について熟知しており、流出サイトにも「クィシン (ゴースト)」という韓国語が含まれている。

Gwisin は、標的型攻撃を仕掛けるランサムウェアだ。これまで世間にはあまり知られていなかったが、2022年 7月頃から、韓国メディアの記事によりその一部が公に知られ始めた。報道によると、Gwisin は 2022年に 5社以上の韓国企業を標的に攻撃を敢

行したが、詳細な侵入方法は明らかになっていない。アンラボは、2022年 8月に初めて顧客企業への被害が報告され、自社の ASEC ブログ内にて関連内容を公開している。

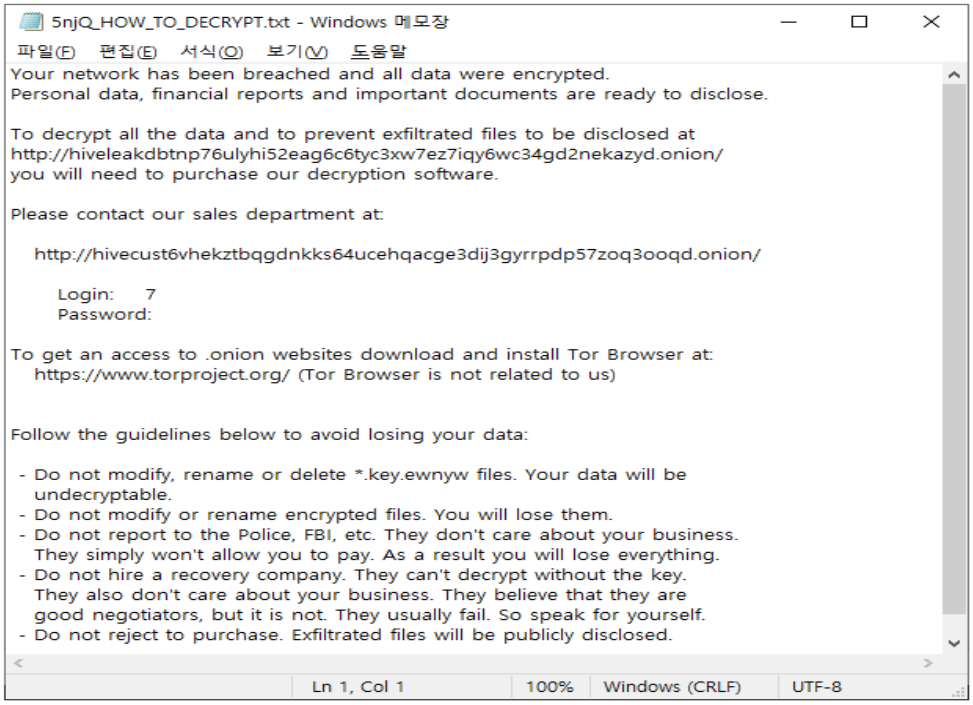
攻撃過程を見てみると、まず内部システムの掌握後、ファイル配布プログラムを利用し不正な MSI ファイルの流布を行う。MSI ファイル内には Binary.helper ファイルが存在し、実行には引数（SERIAL, LICENSE, SMM, ORG）を必要とする。

また、"!!!_HOW_TO_UNLOCK_(企業名)_FILES_!!!.txt" というランサムノートには、英文で被害企業名や流出情報などが記載され、復号化キー・情報公開・脆弱性などの交渉材料をもとに、3段階に渡って交渉を進めるのが特徴に挙げられる。

4. Hive

Hive ランサムウェアは、初めて報告された 2021年 6月から現在まで、その活動を活発に続けている。情報流出およびランサムウェア感染などの二重脅迫型で攻撃を行い、ランサムウェアの復号化に向けた金額交渉が成立しない場合、Hive のリークサイトである「Hive Leaks」に奪取した情報を公開する。米連邦捜査局（FBI）は 2021 年 8月、Hive ランサムウェア組織による活動に対し警告を発表した。

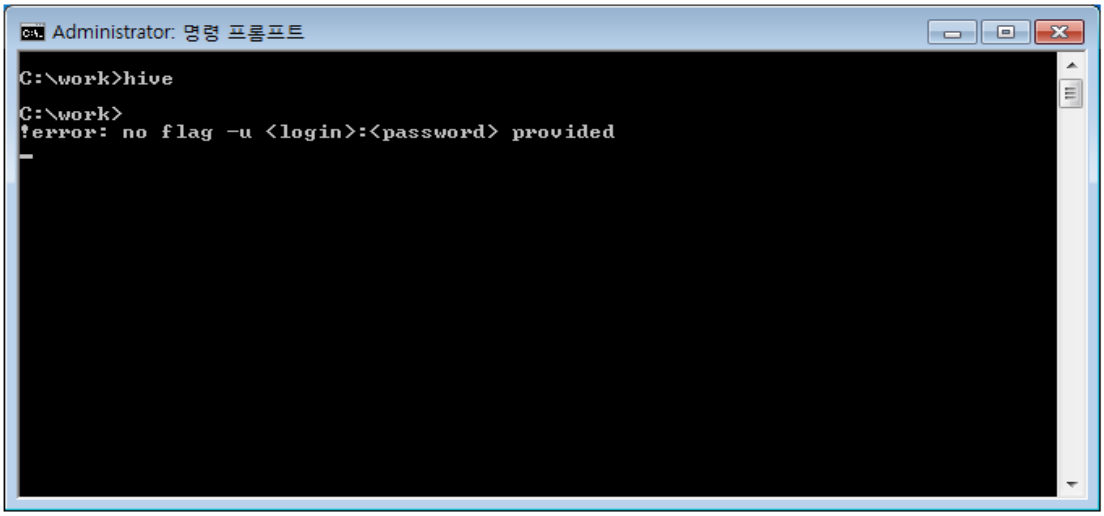
彼らの特徴を見ていくと、2021年 10月に Linux および FreeBSD システムを対象とするバージョンが発見された。初期の頃は Go 言語で作成されていたが、2022年 7月以降は 使用言語が Rust に変わっている。ランサムウェアを感染させた後、被害者側にアクセス可能なアドレス、およびログイン情報が記載されたランサムノートを残すのが特徴だ。



[図2] Hive ランサムウェアのランサムノート

Hive ランサムウェアは、フィッシングメールや ProxyShell など、Exchange Server の脆弱性（CVE-2021-34473、CVE-2021-34523、CVE-2021-31207）を悪用して侵入する。RDP を利用し、内部侵入および内部システムを掌握後、Cobalt Strike ビーコンを介しシステムを制御することで、ランサムウェアを流布する。

最近確認された変型は、実行する上で引数値を必要とし、サンプルのみでの分析が困難となっている。



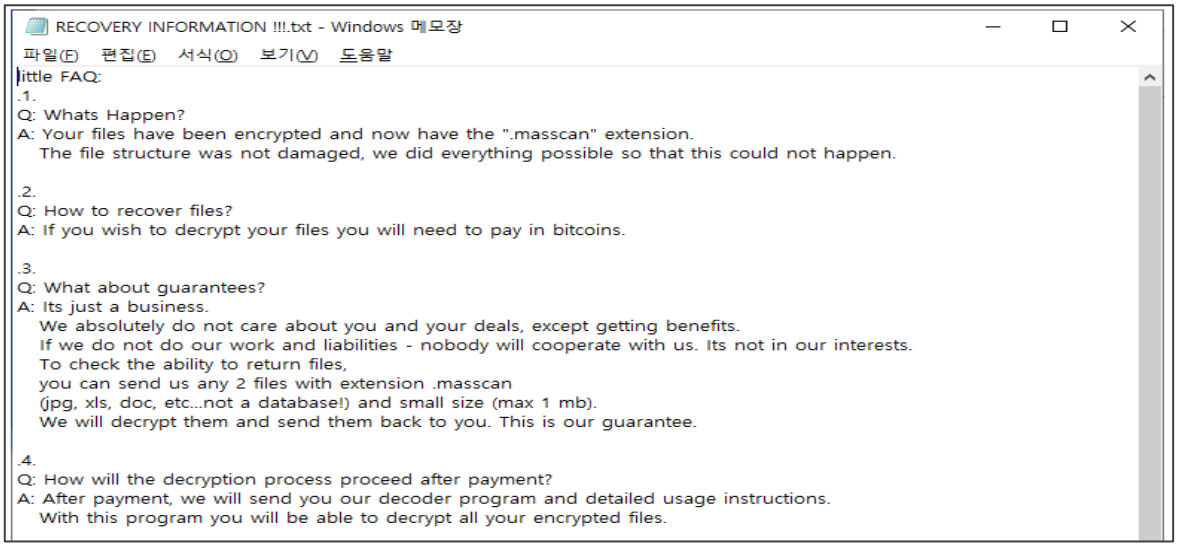
[図3] 引数値のない Hive ランサムウェア実行画面

5. Masscan

Masscan は、2022年 6月から韓国内で活動しているランサムウェア組織であり、現時点で韓国以外の国家での活動は確認されていない。

韓国インターネット振興院（KISA）によると、脆弱なデータベースサーバーを攻撃し侵入することがわかっている。ファイルを暗号化する際、”masscan_アルファベット_ランダム8文字 拡張子” を追加する特徴を持ち、Masscan ランサムウェアと呼ばれている。また、発見された変型では、F・G・Rなどのアルファベットが追加されていた。

[図4] のように、Masscan の場合、ランサムノートとして “RECOVERY INFORMATION !!!.txt” ファイルを生成する。



[図4] Masscan のランサムノート

さらに、ファイルを実行するには設定ファイル（setting.asd）を必要とするが、この設定ファイルに関しては未だ確認されておらず、実行への完全再現には至っていない。

6. LockBit

2019年、初めて公に知られた LockBit ランサムウェアは、アップデート版のバージョン 2.0 に関する流布が、2021年 6月に確認された。バージョン 2.0 では、AD グループポリシーを悪用することで、Windows のドメイン全体を暗号化する機能が追加されている。

以前は、ファイルの暗号化後、拡張子を ".abcd" に変える手法をとっていたことにより、「ABCD ランサムウェア」として名が知られていた。LockBit ランサムウェアの場合、2019年頃から、アメリカ・中国・インド・インドネシア・ウクライナ、およびヨーロッパ諸国に属する組織を対象に攻撃を敢行している。LockBit ランサムウェアもやはり、RaaS 形態で運営が行われており、韓国内では履歴書などを装ったメールの流布、および企業を標的にした攻撃を並行している。

2022年 7月には LockBit 3.0 が登場し、彼らの活動は現在に至るまで衰えを知らない。さらに、LockBit 組織は LockBit 3.0 を公開後、ランサムウェアに関するバグ発見者に報奨金を支払う、「バグバウンティ (Bug Bounty)」制度を導入したことで注目を浴びている。

LockBit の特徴として、ファイルを暗号化する際に多数のスレッドを使用し、各ファイルにつき 4KB 相当のデータのみを暗号化する点が挙げられる。また、Hive ランサムウェアと同様に、実行する上で引数値も必要とする。

セキュリティ製品の無効化および迂回への試み

基本的に、企業のパソコンやサーバーにインストールされたセキュリティ製品およびセキュリティシステムは、攻撃を防ぐ役割を担う。ランサムウェア攻撃による被害が拡大するにつれ、近年のセキュリティ製品は、ファイルの暗号化と推測される行為の遮断、暗号化時の原本ファイル復旧などの機能をもとに、ランサムウェア対策を具現化している。攻撃者の立場からすると、セキュリティ製品に備えられた“アンチランサムウェア” 機能は、攻撃を成功させる上で克服すべき挑戦課題でもある。そのため、セキュリティ製品の無効化や、セキュリティ機能を迂回すべく様々な方法を試みている。

1. セキュリティ製品の無効化

攻撃者側がセキュリティ製品を無効化できる場合、ワクチン診断で予防可能なランサムウェアを用いての攻撃も成功させてしまう。そのため、攻撃者はシステム権限を掌握後、セキュリティ製品のリアルタイムおよび行為監視機能の無効化、もしくはプログラム自体の排除を行う。さらに、Windows Defender や有名なセキュリティ製品を無効化する際に、正常ドライバが用いられることもある。

こうした攻撃を予防するには、組織レベルでワクチンを正しく設定し、できる限り個人ユーザーが設定を変更できないようにする必要がある。

2. セキュリティ製品の迂回

攻撃者がセキュリティ製品を無力化できない場合、彼らはセキュリティ機能の迂回を試みる。

一般的に、攻撃者はランサムウェア製作者からランサムウェアを提供してもらうか、ジェネレータを用いてランサムウェアを製作するが、セキュリティ製品で診断可能なランサムウェアを使用し攻撃するケースも発生している。攻撃者がランサムウェアを実行後、セキュリティ製品に 2回遮断されると、ランサムウェアファイルを暗号化することでローダーを作成し、メモリ内にてランサムウェアを実行する手法が使われた事例もある。

また、セキュリティ製品には、おとりファイルを作成し、該当ファイルが変造された場合、ランサムウェアを検知する機能が搭載されている。しかし、一部のランサムウェアは、セキュリティ製品のインストール経路やセキュリティ製品内に作成されたおとりファイルを、暗号化の段階にて除外する形で迂回を行う。

さらに、BlueCrab・Black Basta などのランサムウェアは、Windows をセーフモードで起動し暗号化を実行する。セキュリティ製品による行為監視機能が有効な状態では、暗号化を行う際に検知・遮断される可能性があるため、強制的にセーフモードで再起動させるのだ。この場合、セキュリティ製品は作動しないため、ランサムウェア攻撃を邪魔されることなくファイルの暗号化が行える。

ランサムウェア攻撃は、セキュリティ製品の迂回により、一度でその攻撃が成功する場合もあるが、1、2回遮断されてからセキュリティ製品を迂回し、侵入してくる場合もある。そのため、セキュリティ担当者は、セキュリティ製品内でランサムウェアに関する診断ログが発生した場合、該当システムおよび感染経路を調査する必要がある。

結論

ランサムウェア組織は、サービス形態が進化するにつれ、徐々にその運営方法が企業化＆分業化されている。ダークウェブ上ではすでに、マルウェア製作者・個人情報の流通・イニシャルアクセスブローカー（Initial Access Broker：IAB)・ランサムウェアの配布・資金洗浄など、各役割が体形的に分業化されている。

だが、特定のターゲットを狙う標的型ランサムウェア組織の攻撃手法に関しては、一般的なハッキング組織と大きな差はない。攻撃者が様々な手法を用い侵入後、内部システムの掌握、および情報を流出させるまでの過程は同じである。その後、情報だけを漏洩させ姿をくらますか、もしくはランサムウェアとして追加攻撃を仕掛けるかに違いがあるだけだ。よって、ランサムウェア攻撃への対策に向けた努力は、その他の攻撃を予防する上でも効果を発揮する。

しかし、予防に向けいくら努力したとしても、ランサムウェアによる被害が発生することもあるだろう。ランサムウェアに感染すると、被害企業の多くは身代金を支払いシステムの復旧を行う。だが、攻撃者の侵入方法を調査・改善しなければ、また別のランサムウェア組織からハッキングされる可能性が出てきてしまう。

従って、ランサムウェア被害が発生した際には、セキュリティ企業に依頼した上で感染経路などの調査を行い、セキュリティシステムの観点から不十分な箇所を改善していく必要がある。また、ダークウェブ上に職員の個人情報およびログイン情報が流出していないか、定期的に確認することも大切だ。ちなみに、企業を攻撃する際、全職員にメールを送信する手法も度々用いられるが、この場合、メールアドレス情報が事前に流出していた可能性が高い。

アンラボはこれまでも、脅威グループの活動を追跡し、関連性のあるマルウェアに対応してきている。彼らの活動が把握されたのが最近だとしても、アンラボの製品ラインナップにて、過去に関連マルウェアを診断している場合がある。しかし、現時点では確認できず、診断に至らない変型マルウェアが存在している可能性もある。

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)