アンラボ・セキュリティレター

Press Ahn

2024.02　Vol.122

実例から学ぶランサムウェア対策

実例から学ぶランサムウェア対策

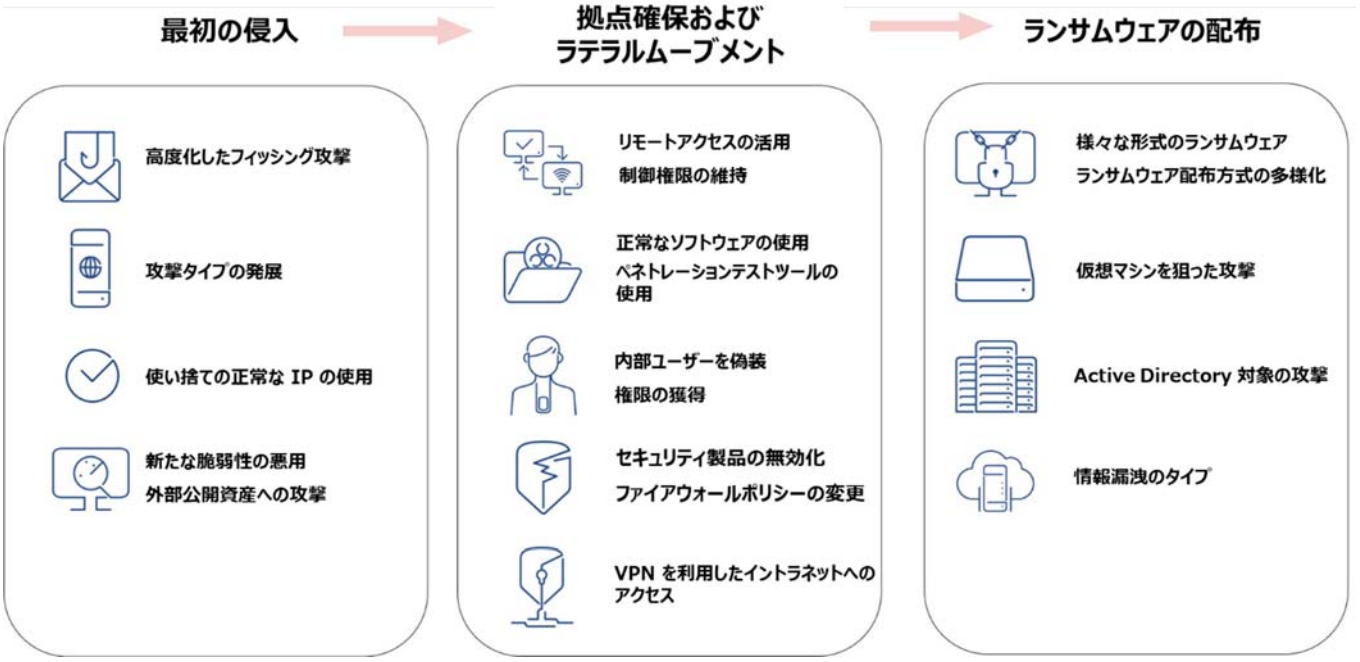
ASEC (AhnLab SEcurity intelligence Center) は、侵害事故の解析後、AhnLab TIP (Threat Intelligence Platform) による侵害事故の解析を通じて得たインサイトをフォレンジックレポートで提供している。

本レポートでは、ランサムウェアによる被害の拡散を軽減するために、ランサムウェアの侵害事故のみを選別し、攻撃者の攻撃手法とランサムウェアの侵害を予防するためのチェック事項を紹介する。

ASEC ではランサムウェアの動向を常時モニタリングしており、月刊レポートを発刊している。AhnLab TIP サービスのサブスクリプションにて、より多様な脅威解析コンテンツを閲覧することができる。

ランサムウェアによる侵害事例から確認された攻撃手法

[図1] は、最初の侵入から拠点の確保、およびラテラルムーブメントやランサムウェアの配布まで、ランサムウェアの攻撃フロー別の主な手法を構造化したものである。



[図1] [図] ランサムウェア侵害の攻撃ポイントと攻撃手法

以下の [表1] は、最近発生したランサムウェア侵害事例において、攻撃者が利用した攻撃手法と特徴をまとめたものである。

詳細項目	攻撃に活用された事例
高度化した フィッシング攻撃	**- より洗練されたフィッシングメールのコンテンツ** ● 正常なユーザーを詐称 ● AI を利用した精巧なコンテンツの制作
使い捨ての正常な IP アドレスの使用	**- 攻撃者と特定するのが困難な正常な IP アドレスの使用** ● 海外のインターネットサービスプロバイダ (ISP) IP アドレス ● 匿名の VPN IP アドレス ● クラウド IP アドレス **- 攻撃に利用された IP アドレス は再利用しない**
VPN を利用したイントラネットへのアクセス	**- マルチファクター認証 (MFA) が適用されない VPN デバイスを利用したイントラネットへのアクセス**
新たな脆弱性の悪用	**- ゼロデイ、ワンデイ脆弱性を積極的に活用** ● セキュリティパッチが適用されていない脆弱な資産を識別し、攻撃を実行 **- サービスの脆弱性を利用したシステムへのアクセス** ● MS Exchange Server の脆弱性を利用したシステムへのアクセス ● Atlassian Confluence の脆弱性を利用したシステムへのアクセス
外部公開資産への 攻撃	**- 外部に公開されたリモートデスクトッププロトコル (RDP) ポートで「Brute Force」攻撃** ● Windows 管理者アカウント (Administrator)

リモートアクセスの活用	**- 攻撃者は GUI 制御権限を好む** ● Reverse RDP ● Google Chrome Desktop ● Team Viewer
制御権限の維持	**- バックドアファイルを自動実行に登録** **- 遠隔制御プログラム（TeamViewer）** **- トンネリングツール（LCX、Plink）** **- Web シェル**
ペネトレーションテスト ツールの使用	**- ペネトレーションテストツールを攻撃手段として使用** ● BloodHoundAD ● Cobalt Strike ● AveMaria RAT を利用したシステム制御
正常なソフトウェアの 使用	**- 攻撃時、正常なソフトウェアを悪用** ● NirSoft プログラム ● Netscan ● PsExec ● Plink ● Lcx ● Team Viewer ● MEGA Cloud ● Rclone ● ADfind ● TreeSizeFree ● ProcessHacker ● dControl
AD 環境を対象	**- アクティブディレクトリ（AD）インフラ情報の収集** ● ADfind **- AD 管理者アカウントの情報があるシステムの探索** ● メモリ内の AD 管理者アカウント情報の収集
権限の獲得	**- ローカル/ドメイン管理者資格情報の収集** ● Mimikatz を利用したメモリ内の資格情報の窃取 ● NirSoft のユーティリティを利用した資格情報の窃取 ● 商用キーロガー（refog）を利用したキーロギング
セキュリティ製品の 無効化	**- システムにインストールされたセキュリティ製品識別の試み** **- GUI 制御を利用してセキュリティ製品サービスの停止および削除**

	● インストールされたアンチウイルスソフトの削除（uninstall） ● dControl を利用した Windows Defender の無効化
ファイアウォール ポリシーの変更	**- ローカルファイアウォールポリシーの変更** ● 特定のサービスポート（445、3389）ポリシーの許可
様々な形式の ランサムウェア	**- ランサムウェアの実行ファイルタイプの多様化** ● EXE、DLL、PS1、MSI のようなファイルタイプのランサムウェア
内部ユーザーに偽装	**- 内部ユーザーと攻撃者を区分しづらくする振る舞い** ● RDP ● SSH ● SMB ● WMIC
仮想マシンを狙った 攻撃	**- 一般のファイルに代わり仮想マシンを狙ったランサムウェア攻撃の増加** ● 仮想ディスクファイル（VMDK）を狙ったランサムウェア攻撃 ● ESXi サーバーを狙ったランサムウェア攻撃
ランサムウェア 配布 方式の多様化	**- 共有ドライブで拠点のシステムに接続し、多数のシステムファイルを一括暗号化** ● sshfs を利用し、Linux システムのボリュームを Windows システムにマウントしてランサムウェアで暗号化 ● net share を利用し、他のシステムのボリュームマウントおよびファイルを暗号化 **- ランサムウェアのリモートコマンドの実行** ● 共有ドライブでランサムウェアをダウンロードおよび実行 ● wmic を利用し、ランサムウェアファイルをダウンロードおよび実行 ● bat ファイルで多数のシステムに一括でコマンドを伝達 **- AD サーバーの IIS サービスを利用したランサムウェアの配布** ● IIS サービスの有効化および Web サービスを利用したランサムウェアの配布 **- AD グループポリシーを利用したランサムウェアの配布**
情報収集	**- データ流出のために、重要なデータ情報を収集** ● TreeSizeFree
情報漏洩のタイプ	**- 外部データクラウドサービスへのデータ漏洩** ● Mega **- 攻撃者のサーバー（C2）へのデータ漏洩**

[表1] ランサムウェア攻撃の手法および活用事例

ランサムウェアの侵害事例

次に、アンラボのデジタルフォレンジック専門組織「A-FIRST (AhnLab Forensic Intelligence ReSearch Team) 」のランサムウェアに関連する侵害事故のフォレンジック解析事例のうち、意味のある事例を選別して簡単に確認していく。

各事例に関する詳しい内容は、同様に AhnLab TIP サブスクリプションサービスでも確認できる。

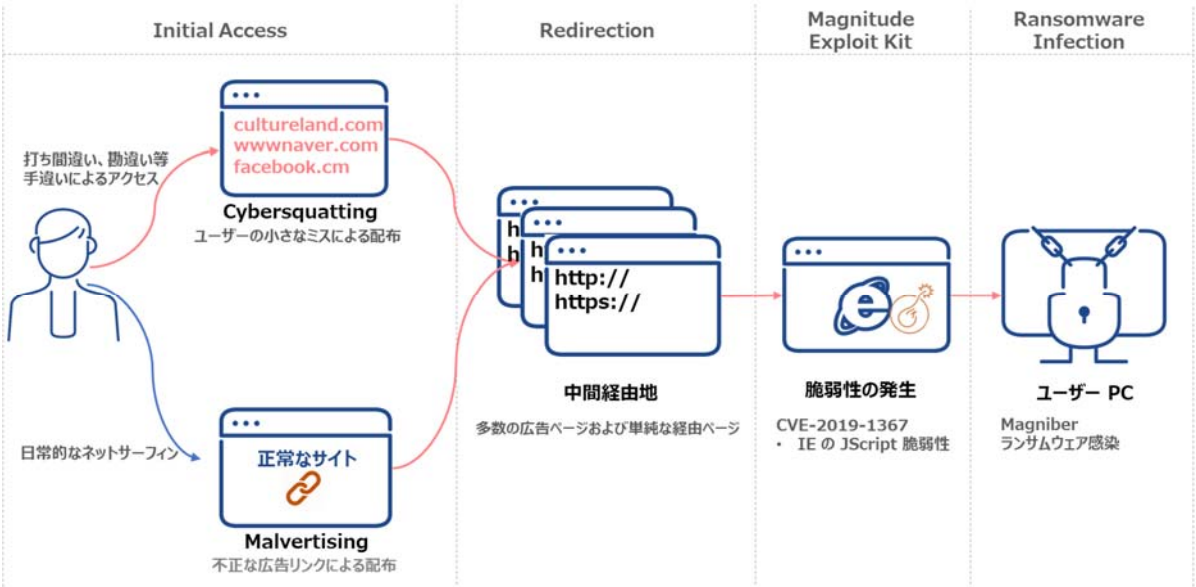
Case 1 : Cobalt Strike を利用した AD 環境の攻撃事例

2019年、TA505 攻撃グループが国税庁の税額計算書等書を装ったスピアフィッシングメールを大量に配布した。攻撃者は、Windows の AD を使用する企業を対象に攻撃を実行し、Cobalt Strike を利用して企業内のシステムを掌握し、ドメイン管理者権限を確保した。幸いランサムウェアの拡散までには至らなかったが、攻撃を試みるプロセスを確認することができた事例である。

*参考 : *Cobalt Strike* はペネトレーションテストのシミュレーションツールだが、攻撃者が好んでよく使用する攻撃ツールでもある。

Case 2 : サイバースクワッティングサイトへのダイレクトアクセスによる Magniber ランサムウェア感染事例

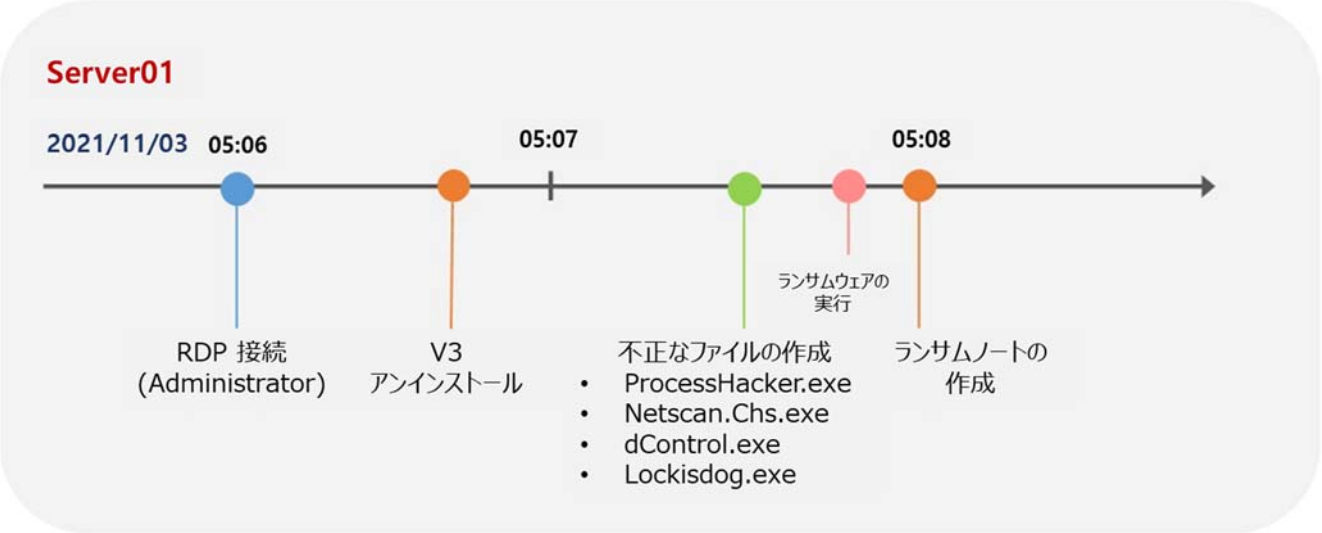
サイバースクワッティング (Cyber Squatting) とは、インターネットのドメインを先取りし、あらゆる利得を得ようとする行為を意味する。攻撃者は、打ち間違いが頻繁に発生するドメイン名を事前に取得しておき、被害者が不正なページにリダイレクト (redirect) するように準備する。ユーザーが URL を入力する過程で打ち間違いが発生すると、攻撃者が用意した不正な Web サイトに接続することになる。



[図2] サイバースクワッティングサイトへのアクセスによる Magniber ランサムウェアの感染プロセス

被害者は複数回のリダイレクトを経た後、インターネットエクスプローラー (Internet Explorer) の JScriptの脆弱性によってランサムウェアに感染する。一般的に不特定多数を狙った攻撃だが、特定組織のドメインに類似したドメインを先取りする方式により、特定の組織を対象としても攻撃が可能であることを確認できた事例である。

Case 3：企業のアンチウイルス管理ポリシーが不十分だったことによる Lockis ランサムウェア感染事例



[図3] Lockis ランサムウェアの感染プロセス

攻撃者は AD の管理者権限を確保し、RDP を通じてラテラルムーブメントを実行した。GUI 権限を持つ攻撃者は、被害システムにインストールされたアンチウイルスプログラムを直接削除し、Lockis ランサムウェアファイルを実行した。攻撃に使用されたランサムウェアファイルはアンチウイルスで検知可能な不正ファイルであるため、アンチウイルスプログラムが削除されていなければ被害を事前に防止できた。アンチウイルスプログラムが任意に削除されないようにする管理ポリシーの重要性を認知することができた事例である。

Case 4：DarkSide ランサムウェア感染事例 - マルウェア感染時、駆除だけにとどめてはいけない理由

攻撃者は AD の管理者権限を取得した後、ドメインコントロール（DC）サーバーで AD のグループポリシーを利用し、ダークサイド(DarkSide) ランサムウェアを配布した。これは、過去2～3年の間に複数の攻撃者による侵害状況が多数確認された事例であり、長期間内部システムが脆弱な状態で晒されていた。セキュリティチェック等を通じて侵害の事実を早くに認知していれば、被害の規模を抑えることができた事例である。

Case 5：Windows Defender を無効化した Hive ランサムウェア感染事例

攻撃者は AD の管理者権限を取得後、共有フォルダーを利用して DC サーバーに Hive ランサムウェアの配布を試みた。しかし Windows Defender によりランサムウェアファイルが検知されると、RDP で直接接続して Windows Defender を OFF にした後、ランサムウェアを実行した。

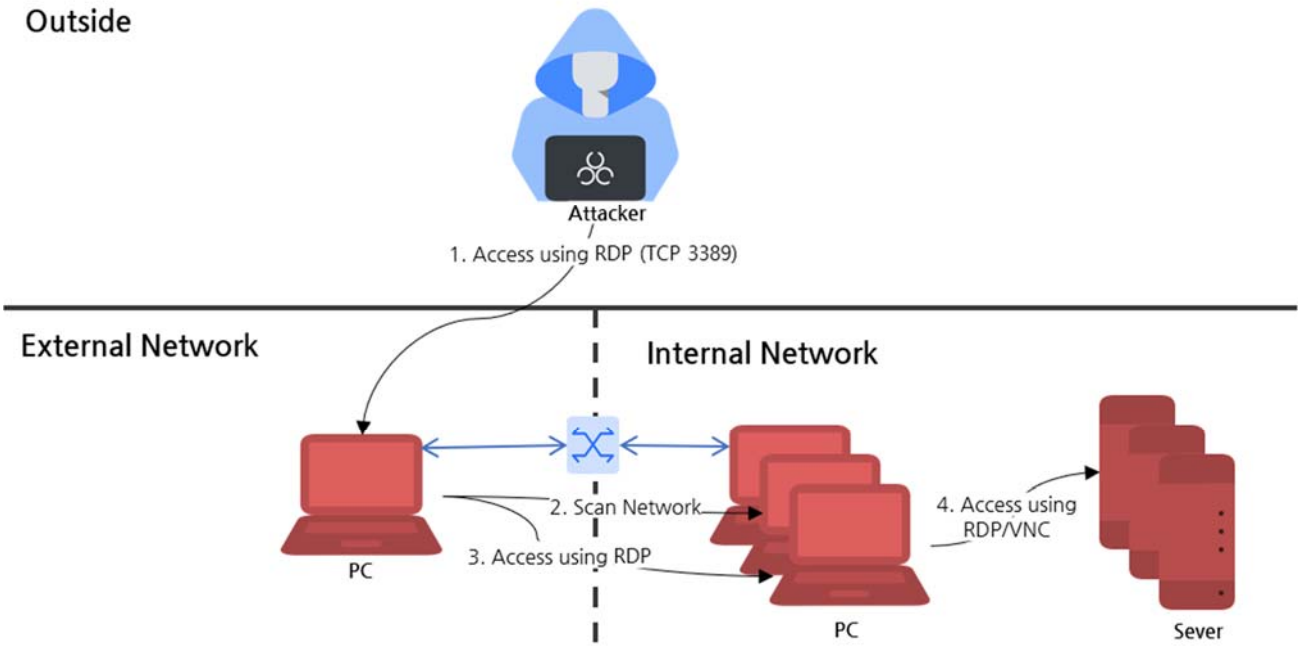
Case 6：韓国国内の企業をターゲットに攻撃を行った Gwisin ランサムウェア感染事例

攻撃者は DMZ 領域に位置するサーバーに Web シェル（WebShell）を挿入した。その後、AD のクレデンシャルを窃取して AD サーバーにアクセスし、AD サーバーに IIS サーバーをインストールした後、 AD に加入しているシステムにランサムウェアを配布した。

Case 7：RDP を通じて侵入後、ESXi サーバーを感染させた Crysis ランサムウェア感染事例

攻撃者は Brute-Force 攻撃を通じて企業内のサーバーにアクセスした後、Windows システムで SSHFS（Secure SHell FileSystem）を利用し VMware ESXi サーバーをマウントしたあと、Crysis ランサムウェアを実行した。攻撃者は暗号化の対象として VMware の仮想ディスクファイルが含まれた仮想ディスクを狙った。Linux サーバーのファイルシステムを Windows システムに接続して Windows 用のランサムウェアで暗号化を行った事例である。

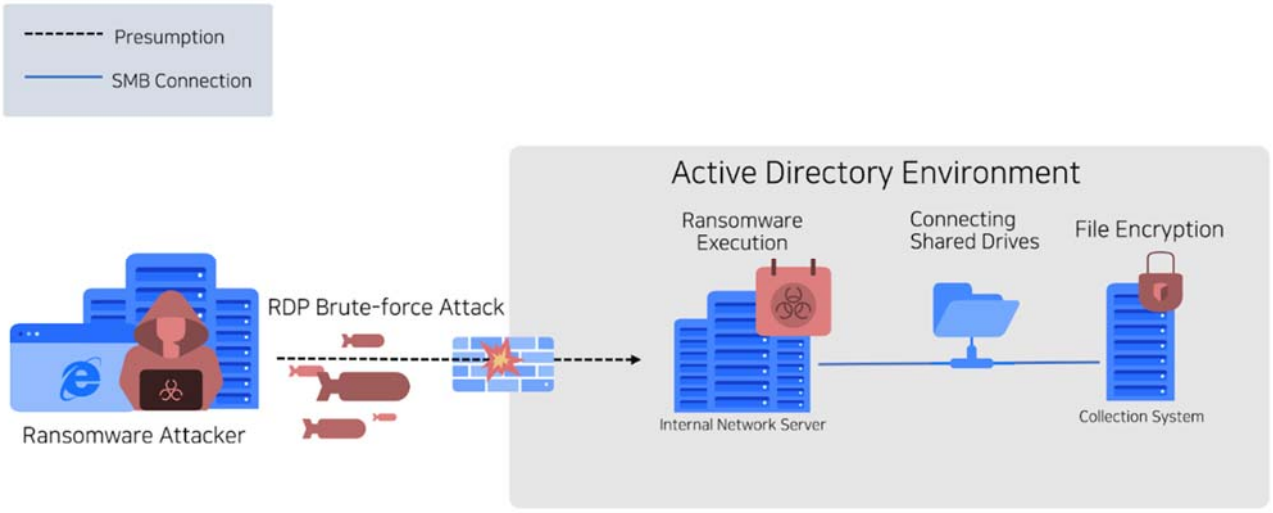
Case 8：RDP の公開と安易なパスワードの組み合わせはランサムウェアを呼び寄せる



[図4] 攻撃者の内部アクセスフロー図

攻撃者は、外部のインターネット環境に RDP が公開されている対象を確認し Brute Force 攻撃でアクセスに成功した後、内部偵察によってさらに RDP でイントラネットのシステムにアクセスした。同じパスワードに設定された管理者アカウントを利用して内部の主要ネットワークへと被害が拡散した事例である。

Case 9：共有ドライブによるランサムウェア感染事例



[図5] 共有ドライブによるランサムウェア攻撃

攻撃者がすべてのシステムにランサムウェアを配布する方式に代わり、少数の拠点となるシステムから多数のシステムを共有ドライブに接続し、ランサムウェアを配布した事例である。

Case 10：Atlassian Confluence の脆弱性を悪用したワンデイ攻撃

攻撃者は Atlassian Confluence の脆弱性 (CVE-2023-22515、CVE-2023-22518) を利用した攻撃を試み、

C3RB3R ランサムウェアを配布した。最近 Atlassian Confluence 製品の脆弱性が相次いで公開され、Atlassian Confluence の脆弱性パッチが適用されていなかったり、最新パッチの管理が不十分なサーバーを対象にワンデイ攻撃が行われた事例である。

ランサムウェアによる侵害を予防するためのチェック項目

ランサムウェアによる侵害に関連する事例において攻撃者が利用した攻撃手法を解析し、ランサムウェアによる侵害を予防するためのチェック項目を選定した。これらの項目をチェックし、攻撃者の侵入難易度を高めて侵害の可能性を低下させ、攻撃プロセスの時点で検知される確率を高めることで、侵害が発生する前に遮断が可能になることが期待される。

分類	チェック項目	詳細内容
ポリシー管理	管理者アカウントの権限管理	**- 不要な管理者アカウントの削除** **- 管理者権限アカウントは最小限の人員にのみ付与**
	パスワード管理	**- デフォルト/共用パスワードの使用禁止** **- Web ブラウザ内でのアカウント/パスワードの自動入力の使用禁止** **- パスワードのヒントにパスワードを明示することを禁止** **- AD 管理者アカウントを認証した PC では、作業後にシステムを再起動** ● メモリ内の認証情報を削除
	外部に公開されている領域の管理	**- 不要な公開領域の削除および最小化** ● サービス用途以外の外部公開を最小化 **- アクセス制限が必要な場合、最小権限に設定** ● 最小権限で定められた期間内のみ許可 ● 定期的なアクセス制限リストの管理が必要
	共有ドライブ設定管理	**- デフォルトでの共有設定を無効化**
	リモートデスクトップ設定管理	**- リモートデスクトップサービスの無効化** **- リモート管理が必要なサーバー資産は別途管理、アクセス可能なシステムを制限**
	ファイアウォールポリシーの管理	- **攻撃に利用可能なプロトコルの通信を無効化する方向でポリシーを管理** ● RPC (135)、SMB (445)、RDP (3389) 等 **- 通信が必要な場合に限り別途許可、およびネットワークのモニタリング** **- 内部サーバー間のアクセス制御ポリシーを設定** ● サーバー間の通信が必要な場合、必要なサービスに限り許可

資産管理	EoS 資産管理	**- サービスのサポートが終了した OS、アプリケーション、サービスのアップデートを勧告** **- アップデートが避けられない場合は別途モニタリングが必要**
	脆弱性のモニタリングおよび管理	**- セキュリティ勧告、および新たな脆弱性のモニタリングを実施** **- 新たな脆弱性の公開時、脆弱な資産を識別して対応** ● パッチ管理ソリューション（PMS）の導入 **- 既存の脆弱性に関しても、脆弱な資産が新たに発生するかどうかをモニタリングする案の策定**
セキュリティ製品	VPN製品の設定	**- 外部からイントラネットへのアクセス時に使用される VPN 製品の設定チェック** ● 多要素認証（MFA）を必須に設定
	アンチウイルス製品の使用	**- ランサムウェアの検知** ● 既知のランサムウェアファイルの検知 ● V3 の「振る舞いベース検知の使用」ポリシーを使用する際、ボリュームシャドウコピーが削除される時にランサムウェアによる振る舞いの遮断が可能 ● デコイファイルの改ざん時、ランサムウェアによる振る舞いの遮断が可能
	製品セルフプロテクト機能の使用	**- セキュリティ製品のサービス中断/削除を保護する機能を使用するように設定** ● V3 の場合、「ロック設定を使用」機能によって設定変更の遮断、プログラム削除防止機能を提供
	セキュリティの死角地帯の最小化	**- ネットワーク/Zone 内部で発生する振る舞いのモニタリング案が必要** ● ネットワーク/Zone の外部、内部間の通信と振る舞いは従来のセキュリティ製品で大半がモニタリング可能だが、内部/内部同士の通信モニタリングに死角が存在 **- EDR/XDR タイプのセキュリティ製品でセキュリティの死角地帯を最小化**
モニタリング	リモートアクセスイベントのモニタリング	**- システムアクセスのモニタリングを強化** ● 管理コンソール外で発生するリモートアクセスイベントのモニタリングを強化 **- 異常な振る舞いのモニタリングが必要** ● 管理者システム、AD サーバーのような、ネットワークアクセスが比較的自由なシステムは、内部拠点として利用される場合がある
	Outbound トラフィック	**- Outbound トラフィックのモニタリングが必要** ● Reverse Shell またはポートフォワーディングの検知
	Windows Defender イベントのモニタリング	**- Windows Defender 有効化イベントのモニタリング** ● アンチウイルス無効化の試みを検知 ● Windows 環境でアンチウイルス製品をインストール時、Windows Defender が無効化 ● その後、アンチウイルス製品が終了したり削除された場合、Windows

		Defender が再び有効化
災害 復旧	データバックアップ案	**- データバックアップ/復旧戦略の策定** ● サービスのタイプによって、デイリーバックアップ、パッチバージョンによるデータバックアップ等、サービス復旧戦略を設定 **- 仮想ディスク/ハイパーバイザー資産の保護** ● 当該資産を狙った攻撃に備えたバックアップ水準と、侵害時の復旧戦略を設定
	サービス復旧案	**- 災害復旧（DR）案の策定** ● ランサムウェアによる侵害発生時のサービス代替
模擬 訓練	セキュリティ認識の 向上キャンペーン	**- ユーザーを対象とする攻撃で侵害が開始されるケースが多数** ● フィッシングメールの模擬訓練 ● セキュリティ認識教育の実施
	事故対応の 模擬訓練	**- 侵害発生時の迅速な対応のための訓練を実施、および手順の検討** ● APT 事故対応の模擬訓練 ● 災害復旧の模擬訓練

[表2] ランサムウェアによる侵害を予防するためのチェック項目

ランサムウェアによる侵害原因を解析するためのチェック項目

最後に、ランサムウェアによる侵害の発生時に侵害原因を解析するためにチェックすべき項目を選定した。ランサムウェアによる侵害の発生後、原因解析を行うことなく復旧が行われると、同じ原因によりランサムウェアに再感染する場合がある。

したがって、ランサムウェア侵害の発生時に原因を解析することにより、システム内に残存する不正なファイルを識別し、侵害プロセスおよび原因の解析を通じて再発を防止し、システム復旧のための準備が必要となる。

チェック項目	詳細内容
被害システムの 保存手順のチェック	**- ネットワークの切り替え、およびシステム電源を維持した状態で隔離が可能かをチェック** ● 電源を切るとライブ状態のシステムで取得可能な情報が失われるため、できる限り電源を維持したまま隔離
セキュリティ機器の ログ保存期間を確認	**- セキュリティ機器のログは、少なくとも6か月以上保管** ● 最初の侵入からランサムウェアによる侵害まで、数時間、数か月、さらには数年かかるケースもある。 ● 事後解析のために、可能な限り長期間のログを保管 **- VPN 使用時、VPN 使用ログから実際のユーザーを識別可能かをチェック** ● ユーザー識別不可の場合、VPN IP アドレス 割り当て方式をユーザー別の静的割り当て方式を考慮

事故発生時の セキュリティ機器ログの収集	**- 侵害を認知した時点を基準に、収集可能なセキュリティ機器のログを収集** ● セキュリティ機器のログ保存期間が短い場合、侵害を認知した時点で収集可能な情報を事前に収集。

[表3] ランサムウェアによる侵害原因を解析するための点検項目

より多様なランサムウェア解析情報と脅威インテリジェンスコンテンツは、当社の脅威インテリジェンスプラットフォーム「AhnLab TIP」サブスクリプションサービスで確認できる。

►TIP ポータルのショートカット

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)