cisco Secure

サイバー攻撃の被害が大きくなる仕組みを知ろう！ キーワードは「ラテラルムーブメント」

西　豪宏　シニアSEマネージャー

満江 貴之 テクニカルソリューションズアーキテクト

シスコシステムズ合同会社 セキュリティ事業

2021年1月13日（水）

https://gblogs.cisco.com/jp/2020/11/ransomware_defense/

Cisco Japan Blog > セキュリティ

セキュリティ

他人事ではない！ ランサムウェアの脅威とその対策について

西 豪宏
2020年11月25日

コロナ禍につけ込んだサイバー犯罪が増加の一途を辿っている中、Snake, Ragnar Locker などのランサムウェアと呼ばれる脅威と被害が拡大しています。

攻撃者は盗み出したデータを人質に取り、ビットコインなどで身代金（ransom、ランサム）を支払わないとデータを「晒す」と脅迫し、これを支払わなければ機密情報を暴露されるという被害に発展する事例が増えています。

シスコは昨今のランサムウェアの被害拡大を踏まえ、ウェビナーを緊急開催予定です。

本ブログとウェブセミナーでは、ランサムウェアの脅威は何なのかにはじまり、なぜ被害をうけてしまうのかという原因と、どうすれば防ぐことができたのかに関して Cisco Talos インシデント対応チームの対応事例なども踏まえ、対策のポイントをわかりやすく解説いたします。

ウェビナー録画(2020/12/4) :【緊急開催】ランサムウェアの脅威と対応について

ラテラルムーブメント

横断的侵害・侵入後の横展開・侵害範囲拡大・側方移動

lateral（訳）：横への、側面に向かう

第1段階(準備):攻撃者は標的組織への侵入の前に入念に調査し侵入の手筈を整える。
第2段階(潜入):攻撃者は標的組織のセキュリティ防御を破り侵入する。
第3段階(横断的侵害):攻撃者は組織内の侵害を広げ目的とする重要資産に近づく。
第4段階(活動):攻撃者は重要資産に対しデータの窃盗、改ざんなどの行為を行う。

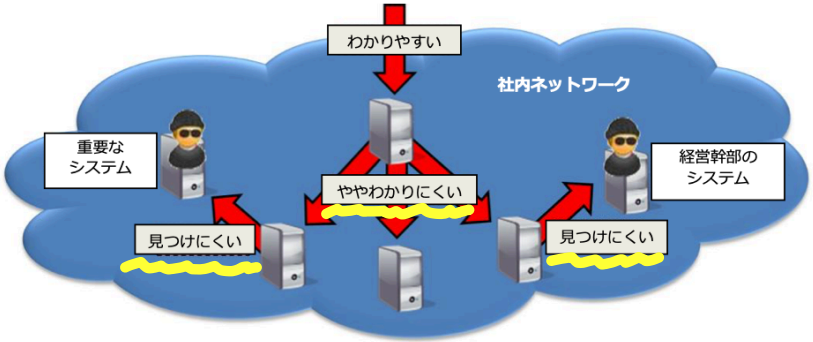
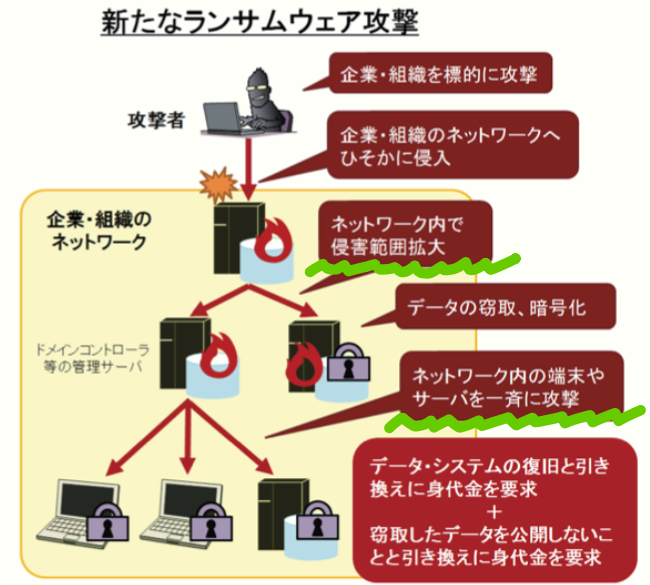


図 5：APT の横断的侵害

出典：JPCERT
高度サイバー攻撃(APT)への備えと対応ガイド(2016/3/31)
https://www.jpcert.or.jp/research/20160331-APTguide.pdf

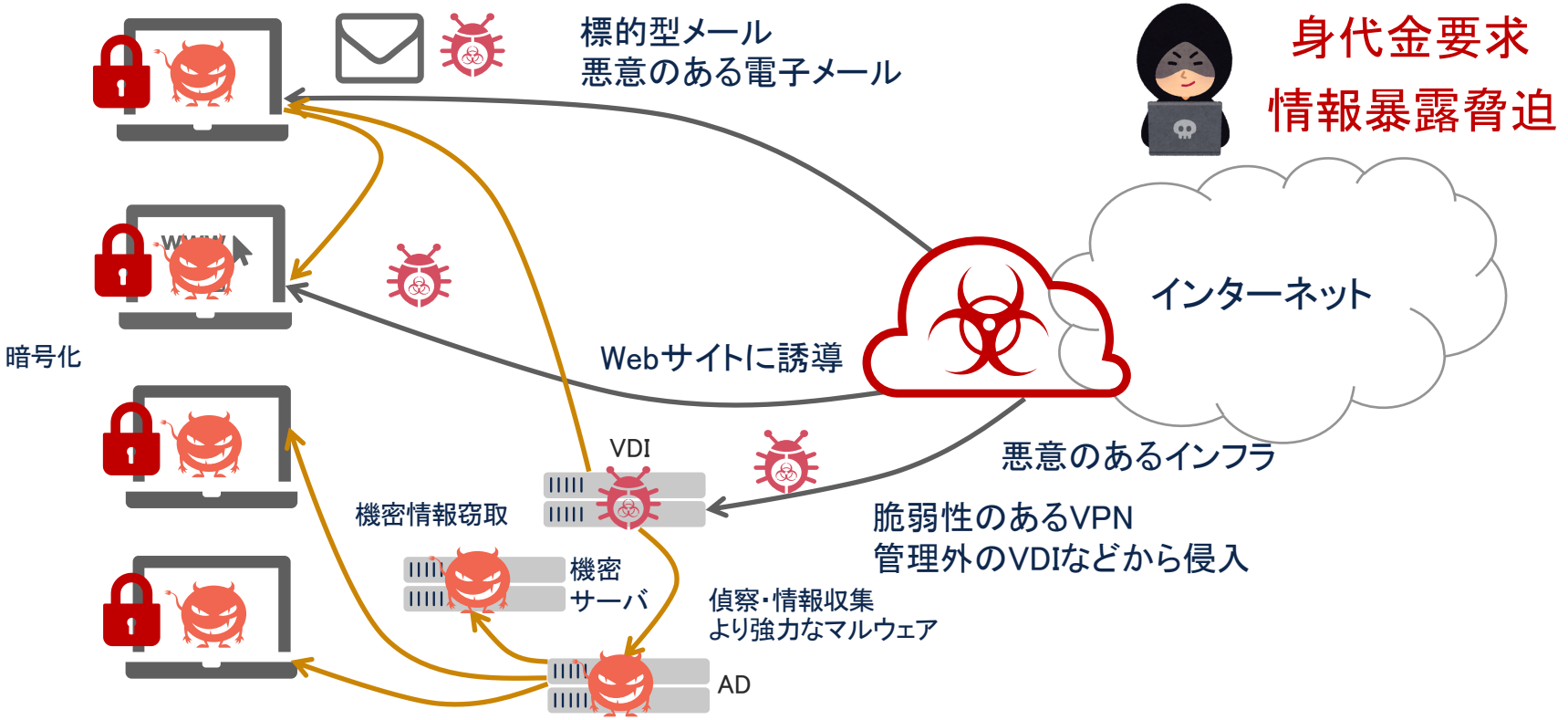
「人手によるランサムウェア攻撃」では、諜報活動を目的とする標的型サイバー攻撃と同様、攻撃者自身が様々 な攻撃手法を駆使して、企業・組織のネットワークへの侵入、侵入後の侵害範囲拡大(側方移動、lateral movement)等をひそかに進める。



出典：IPA
事業継続を脅かす 新たなランサムウェア攻撃 について(2020/8/20)
https://www.ipa.go.jp/files/000084974.pdf

ランサムウェア攻撃のプロセス

ラテラルムーブメントによってサイバー攻撃の被害が大きくなる

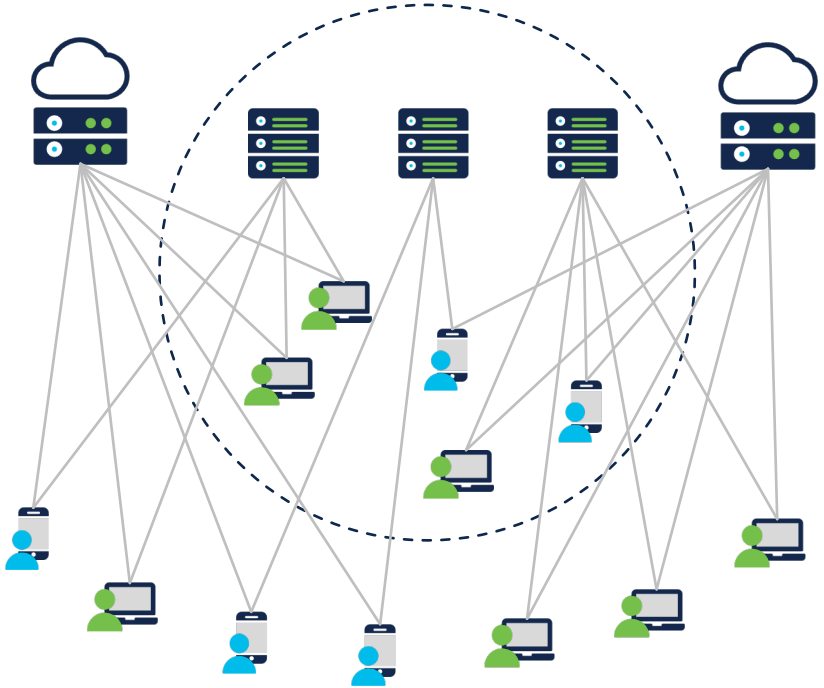


1.侵入開始・初期感染

2.偵察行動・感染拡大

3.実行・被害

環境の変化
ラテラルムーブメントが検知しにくい背景



ユーザ・デバイス環境の変化
- テレワークの増加
- リモートユーザの増加
- IoTデバイスの増加

サービス提供環境の変化
- サーバ分散
- マルチクラウド
- 複雑な通信要件の把握
- 急なサービス拡大
- 新機能の追加

従来型の対策では、攻撃者に侵害されると境界の中は無法地帯となってしまう

ゼロトラストという考え方

境界型セキュリティの限界

多様化するアクセス環境において
- 適切なアクセス権を確保したい
- 拡大する攻撃対象を保護したい
- 広範囲な可視性を確保したい

課題に対処する新しい考え方

場所 ≠ 信頼
場所やネットワークを信頼しない

信頼性の再定義
1度限りの検証に頼らず継続確認する

アクセス制御
最小限の範囲を最小限の時間で制限

自動化ポリシー
可視化された情報を利用したアクセスの調整

ユーザ

アプリケーション

デバイス

データ

継続的な診断

信頼の確立　　信頼に応じた制御

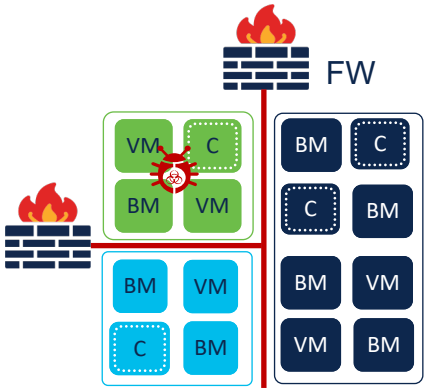
Cisco ゼロトラスト

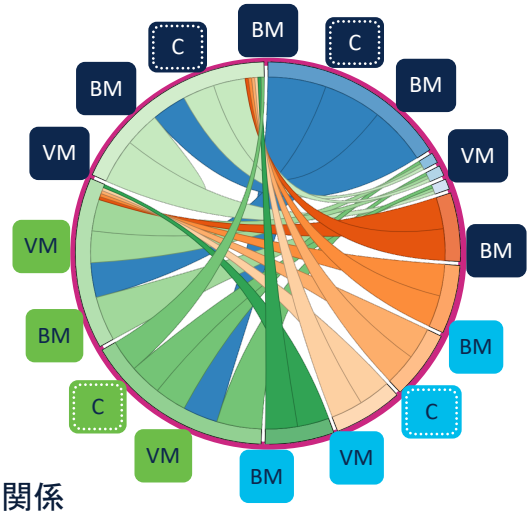
継続的な診断による信頼の確立

ワークロード間の通信を継続的に診断
ラテラルムーブメントを防止する

Group 1 BM Bare-Metal サーバ
Group 2 VM 仮想マシン
Group 3 C コンテナ

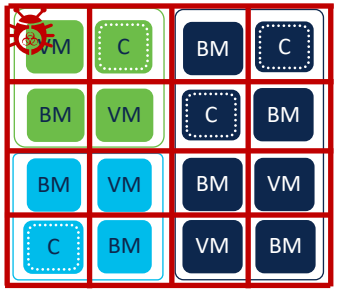
境界内は自由に通信





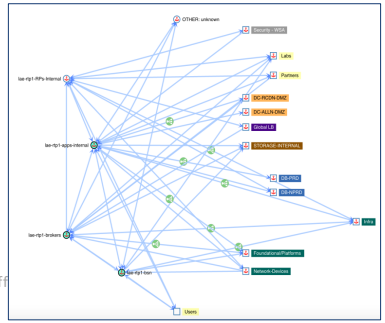
必要な通信のみ許可

Tetration

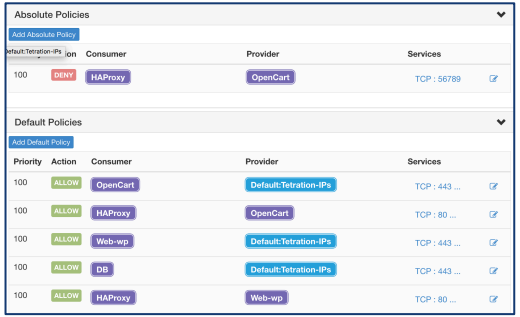


- サーバ分散・マルチクラウド
- 複雑な通信要件
- サービス拡大や機能追加

アプリ依存関係
通信要件の自動収集



ポリシー自動生成



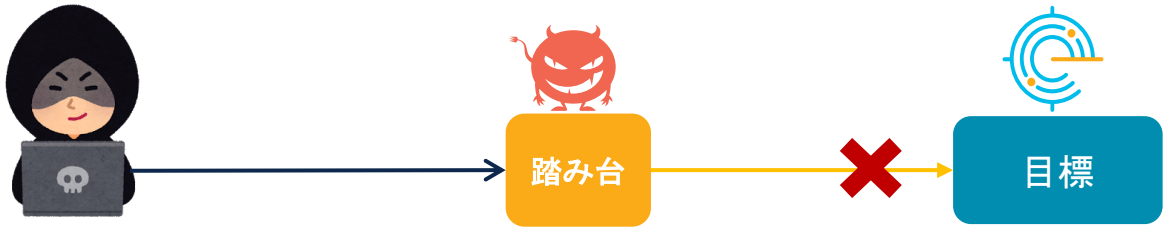
- 環境非依存
- マルチクラウド対応
- リアルタイム学習診断
- ホワイトリスト
- 脆弱性をポリシーに反映

- マイクロセグメンテーション

cisco Secure

Cisco Secure Workload (Tetration) デモ

続きのセッションはデモンストレーション
でのご説明となります



Cisco Secure Workload (Tetration)
マイクロセグメンテーション デモ
ラテラルムーブメントを防ぐ仕組みを御覧ください

ゼロトラスト：継続的な診断による信頼の確立

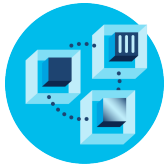
これまでの対策と課題

ユーザ名・パスワード定期的変更

複雑なパスワードで！

- VPN情報乗っ取り犯罪
- 情報を盗まれて侵入される

静的ポリシーでの通信制御



継ぎ足しACLで守る！

- 内部可視化へは未着手
- 侵入後は静的ポリシーの範囲で自由に行動

とにかくマルウェアを検知する

マルウェア検知99%！

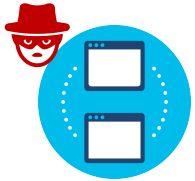
- 特定の標的マルウェア
- 1つの侵入で十分

これからの対策＝ゼロトラスト

パスワードが盗まれても
不審者かどうか
不適切な端末でないか
見極める仕組みが必要

- 多要素認証に加え
- アップデート必要なデバイスをを許可しない
- 10分後の遠隔地でログインブロック
- 突然深夜にログインすると警告

多要素認証
Duo



異常な振る舞いや
疑わしい通信を
検知して対処する
仕組みが必要

- 通信を継続的に診断し、ラテラルムーブメントを防止する

アプリ保護
Tetration

- ネットワーク脅威検知と対処
- 正しいユーザとデバイスを継続的に診断

脅威検出
StealthWatch

脅威収集・隔離
ISE

感染が広がっても
初期感染者や
どこまで広がっているか
の把握して対処する
仕組みが必要

- マルウェアを継続的に可視化して、ネットワークレベルで制御

マルウェア対策
AMP/TG

脅威収集・隔離
ISE

信頼の確立・信頼に応じた制御・継続的な診断

cisco Secure

まとめ

高度化するサイバー攻撃

- コロナ禍につけ込むサイバー犯罪は急増し、標的型攻撃やランサムウェアの脅威や被害が拡大しています
- 攻撃者は巧妙に侵入し、目立たないようにひそかに内部の情報収集を行い目的を達成します

なぜサイバー攻撃の被害が大きくなるのか

- 最初の侵入から実際に被害をうけるまでに、攻撃者は攻撃の成果を最大化するためにラテラルムーブメント（侵害範囲拡大）という手段でより広範囲な対象や、より価値のある情報を狙います
- ラテラルムーブメント（侵害範囲拡大）は一般的なセキュリティ対策を潜り抜けるように攻撃を進めるため、攻撃の進行を検知しにくく、判明した時点では既に大きな被害が生じている場合があります

データとアプリケーションも含めたゼロトラストという考え方で防ぐ

- リモートワーク増加によりユーザ・デバイス環境の変化や、クラウド利用促進によるサービス提供の環境の変化のなか、多様化するアクセス環境において、ゼロトラストという考え方が必要になっています
- サイバー攻撃被害拡大が大きくなるのを防ぐためにはデータやアプリケーションの通信を継続的に診断する、ラテラルムーブメントを防ぐ対策が効果的となります


cisco
Secure