VECTRA
SECURITY THAT THINKS

インシデント事後分析レポート

ランサムウェアオペレーションを事前に阻止する

目次

Vectra®は、サイバー攻撃をいち早く検知して阻止することで、ビジネスの安全性を担保します。

ネットワーク上の脅威の検知および対応（NDR）におけるリーダーであるVectraは、皆様のデータやシステム、インフラストラクチャーを保護します。SOCチームは、Vectra製品によって攻撃者の振る舞いを事前に検知し、適切な対応を取ることができるようになります。

オンプレミスかクラウドかに関わらず、ネットワーク上の不審な振る舞いや行動を幅広く迅速に検知します。また、セキュリティ担当者が迅速に対応できるよう、攻撃を検知・識別してアラートを発信します。

Vectra製品は、「自ら思考するセキュリティソリューション（Security that thinks®）」を実現します。人工知能を駆使することによって、時間の経過と共に検知と対応能力が向上し、誤検知を排除して実在する脅威に集中できるようになります。

お客様：製造業

エグゼクティブサマリー

2021年6月13日（日）、製造業のお客様からの緊急サポート依頼を受け、VectraのSidekickチームが出動しました。担当アナリストがお客様側のチームと密に連携しながらVectraの検知機能と収集データを活用して攻撃の進行を阻止し、修復対応を行いました。

- **Vectra Detect for Networks：**AI駆動型の検知、優先順位付け、自動対応により、攻撃の進行をその場であぶり出して阻止。
- **Vectra Recall™：**ネットワーク全体のメタデータを提供し、調査・インシデント対応から攻撃者撃退までのプロセスをサポート。

インシデントの事後分析によって、この攻撃がランサムウェアFiveHandsに関与するグループ「UNC2447」の仕業だったことが示唆されています。攻撃は、データの持ち出しやランサムウェアのペイロードがデプロイするに至る前に食い止められました。

攻撃者は長期間におよぶ外部偵察フェーズを経て、標的組織の業務時間外に、SonicWallのVPN経由でネットワークにアクセスしました。当該アクセスから2分以内にVectraが攻撃活動を特定し、コンソール画面に表示された攻撃元ホストの優先度を「Critical」に分類しました。

同日夕方にかけて侵入が進み、ドメインコントローラ内のドメイン管理者権限が奪取された時点でVectraの自動対応機能が発動し、連携先のEDR経由で当該ホストのさらなる活動を食い止めました。セキュリティ担当チームの迅速かつ迷いのない判断とフォローアップにより、ランサムウェアのデプロイリスクを払拭したうえで、協力相手のインシデント対応チームが余裕をもって調査を行い、攻撃者を撃退することができました。

今回の事案では、スピーディーな検知と迷いのない対応（ツール、人材、テクノロジー）が成功の鍵となりました。活発な攻撃は、現地時刻の18:01（業務終了直後）からスタートしています。たとえ数時間でも対応が遅れていれば、ほぼ確実に同日夜間にランサムウェアがデプロイされていたでしょう。さらに攻撃者はVeeamのバックアップ構成ファイルを指定して検索し、保管場所を特定していました。バックアップを破壊し、身代金を支払わなければファイルを修復できないようにする意図もあったと思われます。

外部偵察活動（6月8日～12日）

偵察活動を示唆する最初の証拠は、攻撃者がVPN、FTP、Webメールをはじめとする複数のサービスの探索（プローブ）を始めた2021年6月8日に検知されました。発信元はロシアのIPサブネットでした。

VPNインタラクションの推移

その翌日（6月9日）、複数のターゲットに対するHTTP GETおよびHTTP POSTリクエストの証跡がVectraによって確認されました。ターゲットシステムの背後にあるApacheサーバーの脆弱性をチェックする目的と見られます。

HTTPリクエストには、標的組織の環境内で独自のユーザーエージェントが使われていましたが、これとは別に、2021年6月3日の08:01に同じユーザーエージェントを使ってリクエストを実行した外部IPアドレスが存在していました。当該アドレスは6月9日にほんの一瞬、アクティブな状態でした。トラフィック量および転送バイト数がごくわずかだったため、攻撃者が誤ってルーティングしたものと見られます。

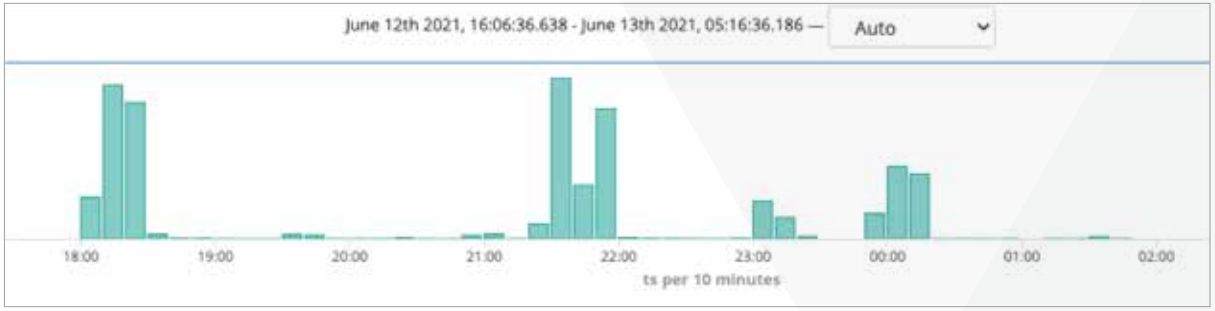
```
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/78.0.3904.108 Safari/537.36
```

独自のユーザーエージェントを確認

初期アクセス（現地時刻6月12日18:01）

18:01 ー 攻撃者はまず、有効なユーザーアカウントがVPNにログインしたと同時に、攻撃元ホストから標的ネットワークにアクセスしました。

アクセス経路はSonicWallのVPN経由でした。SonicWallとのライセンスの問題もあり、お客様環境への多要素認証(MFA) の実装が遅れていたため、MFAはこの時点では有効化されていませんでした。パッチ未適用のSonicWall製品には認証情報の漏えいにつながる脆弱性があるため、これが悪用された可能性が高いものの、裏付けは取れていません。攻撃元ホストには有効なVPNプロファイルも使われていました。つまり、侵害されたユーザーのノートPCからプロキシ接続された、もしくは攻撃者がVPNプロファイルを窃取して自らのインフラ経由で接続した可能性があります。



攻撃元ホストのセッション推移

偵察活動

偵察フェーズの活動はすべて、VPNにログインした攻撃元ホスト（ネットワーク外部のホスト）と同じホストから実行されていました。

接続を確立した攻撃者がDNSリバースルックアップやリモートプロシージャコールなどを使ってネットワークの情報を収集し、積極的な偵察を開始した直後に、Vectraの各種検知項目がその存在を特定しました。詳細は以下のとおりです。

初回ログイン後ほどなく、システムのサブネットIPに対する大量のDNSリバースルックアップが実行されました。この活動は、偵察時の振る舞いと一致しています。

DNSリクエストはこのほか、無料オンライン版の脆弱性スキャナーEternalBlueおよび、プログラミング、倫理ハッカー、侵入テストのオンラインフォーラムに使われるドメインコード（.netが付くドメイン名）に対しても実行されていました。当社チームではこの振る舞いは、攻撃者による脆弱性の特定および、標的環境で実行可能なエクスプロイト手段の選別を目的としたものと考えています。

さらに、yandex.ru、ok.ru、google.ruなどのロシア国内ドメインに対するDNSルックアップの証跡も確認されたため、攻撃者がロシア拠点であることが推定されます。前述の不審なDNSリクエストと合わせて考えると、攻撃者は自らのDNSトラフィックが標的企業のネットワーク経由でルーティングされたことを把握していなかった可能性が非常に高いでしょう。

2.0.5.10.in-addr.arpa	PTR
13.0.5.10.in-addr.arpa	PTR
47.0.5.10.in-addr.arpa	PTR
9.0.5.10.in-addr.arpa	PTR
3.0.5.10.in-addr.arpa	PTR
5.0.5.10.in-addr.arpa	PTR
12.0.5.10.in-addr.arpa	PTR
14.0.5.10.in-addr.arpa	PTR
4.0.5.10.in-addr.arpa	PTR
8.0.5.10.in-addr.arpa	PTR
43.0.5.10.in-addr.arpa	PTR
33.0.5.10.in-addr.arpa	PTR
15.0.5.10.in-addr.arpa	PTR

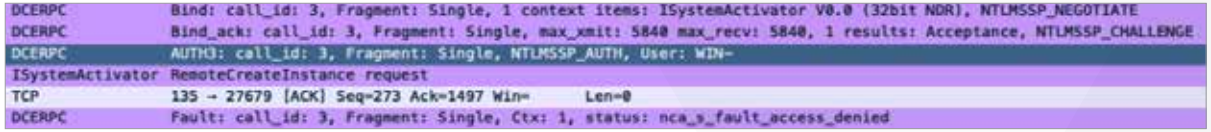
DNSリバースルックアップ

VPNへの初回ログインからわずか2分後の18:03には Vectraの検知項目が5件（下記のとおり）トリガーされ、この攻撃元ホストの優先度がCriticalに分類されました。

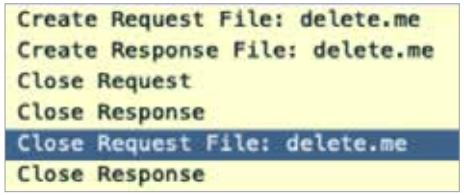
- レプリカの自動作成
- ポートスイープ
- RPCの偵察
- RPCの標的型偵察
- ファイル共有の列挙

検知項目「レプリカの自動作成」では、ホスト10.5.1.20に対して 管理者アカウントで**NTLMSSP__AUTH**を使って認証を試みていた**WIN-XXXXXXXXXXX**という形式のホスト名が特定されました。お客様環境で、こうした汎用形式のWindowsホスト名が使われている場所は他にありませんでした。その後のRDPデータにも同じホスト名が表示されているため、攻撃に用いられたホストに間違いないと考えられます。

また、**delete.me**というファイル名に対する読み取り・書き込みのリクエストがSMB接続を介して送信されていました。これは、偵察ツールの**NetScan**がファイル共有の書き込み権限をチェックする際と同じ振る舞いです。



PCAPによる「レプリカの自動作成」の解析



NetScanの振る舞い

18:16 ― 攻撃者が接続を確立した際、これまでにないパターンでのSMB管理共有へのアクセスをVectraが検知しました。ほどなくして、SMB経由で別のシステムへの接続（パス：\\10.5.0.65\backup_exchange$）も確立され、合計10.9MBのファイルがソース側ホストに転送されました。すでに攻撃元ホストがVPN経由で接続していたため、Veeamの圧縮ファイルが標的組織の外に持ち出されたものと思われます。

21:09 ― 攻撃者がIPアドレス10.5.3.28のホストに対するRDPセッションを確立した際、Vectraが不審なリモートデスクトップ接続を検知しました。接続情報に表示されているソースのホスト名（**WIN- XXXXXXXXXXX**）が、攻撃元ホストに間違いないと考えられます。

21:15 ― 悪質な認証情報ダンプツール**mimikatz.exe**が、2つのシステム（ホスト名は非開示、IPアドレスは10.5.2.12と10.5.3.28）に転送されていたことをVectraが検知しました。転送結果の取得目的でのファイルアクセスについても、証跡が残っています。

June 12th 2021, 18:18:13.126	WIN-[redacted]	\\10.5.0.65\backup_exchange$	[redacted]	SMB::FILE_OPEN	10.5.0.70	10.5.0.65
June 12th 2021, 18:18:13.126	WIN-[redacted]	\\10.5.0.65\backup_exchange$	[redacted]	SMB::FILE_READ	10.5.0.70	10.5.0.65
June 12th 2021, 18:18:13.126	WIN-[redacted]	\\10.5.0.65\backup_exchange$	[redacted]	SMB::FILE_READ	10.5.0.70	10.5.0.65
June 12th 2021, 18:18:13.126	WIN-[redacted]	\\10.5.0.65\backup_exchange$	[redacted]	SMB::FILE_READ	10.5.0.70	10.5.0.65
June 12th 2021, 18:18:13.126	WIN-[redacted]	\\10.5.0.65\backup_exchange$	[redacted]	SMB::FILE_READ	10.5.0.70	10.5.0.65
June 12th 2021, 18:18:13.126	WIN-[redacted]	\\10.5.0.65\backup_ex ge$	[redacted]	SMB::FILE_READ	10.5.0.70	10.5.0.65

Vectraが捉えたSMB接続の証跡

ラテラルムーブメント（横方向の移動）によるドメインコントローラの奪取

偵察活動はすべて、同一ホストから実行されていました。攻撃者が偵察で得た情報を精査していたと思われる2時間程度の小休止を経て、攻撃が次のフェーズ「ドメインコントローラの乗っ取り」に移行しました。

00:25 ー サブネットおよびコンピュータオブジェクトカテゴリの検索と見られる不審なLDAPクエリが2件、攻撃元ホストから実行されていることをVectraが検知しました。

合計1,006個のオブジェクトが返されているため、クエリが成功したと考えられます。こうした振る舞いは通常発生しにくく、ネットワークの偵察活動と一致しています。

00:34 ー ドメインコントローラ(DC1)に対するRDP接続が確認されました。00:41には、2つ目のドメインコントローラ(DC2)に対するRDP接続も確認されました。どちらのセッションでも大量のデータが転送されており、セッションが成功したと考えられます。

不審なLDAPリクエスト

ドメインコントローラへのRDP接続

00:39 ー DC1がネットワークスキャンを開始した際に、以下の検知項目がトリガーされました。

- レプリカの自動作成
- ファイル共有の列挙
- 不審なリモートコードの実行
- ポートスイープ
- SMB管理共有への新種のアクセス
- RPCの標的型偵察
- RPCの偵察

00:41 ー VectraからEDR経由で自動阻止をトリガーしてシステムを隔離し、当該活動を停止させました。

DC2についても、同様のパターン（スキャンの検知、自動対応・自動隔離）となりました。

自動隔離の際にはセキュリティ担当チームも招集。同チームはこの状況をただちに「深刻かつ継続的な攻撃」と判断し、充分時間をかけて調査・修復ができるよう「インターネットの一時遮断」に踏み切りました。

調査および修復

この時点でVectraのSidekickチームが参画し、活動の全容解明および攻撃者撃退までの支援を行いました。

- 侵害が疑われる攻撃元ホストを捕捉し、調査を経てホストを削除。侵害の痕跡は表面化していないため、侵害されたホスト経由のプロキシ接続ではなく、あらかじめ窃取したVPNプロファイルを使って、攻撃者自らのインフラから接続された可能性が高いと思われます。
- 攻撃者がドメインコントローラへの接続を確立していたため、「最悪のシナリオ」（ゴールデンチケットの悪用）を想定して動くことがベストだとお客様側で判断。これを受けてドメインをすべて再構築し、KRBTGTを2回リセットしました。エンドポイント全体のフォレンジック調査にはさらなる時間を要するため、ネットワーク接続をいち早く再開して業務を復旧させるための果断です。
- VPNにパッチを適用し、すべてのアカウントに二要素認証 (2FA) を実装。
- 同じ攻撃者によるさらなる活動を瞬時に検知できるよう、ネットワーク復旧後にカスタム検知モデルを追加し、優先度別に分類しました。

お問い合わせ：info-japan@vectra.ai　vectra.ai/jp