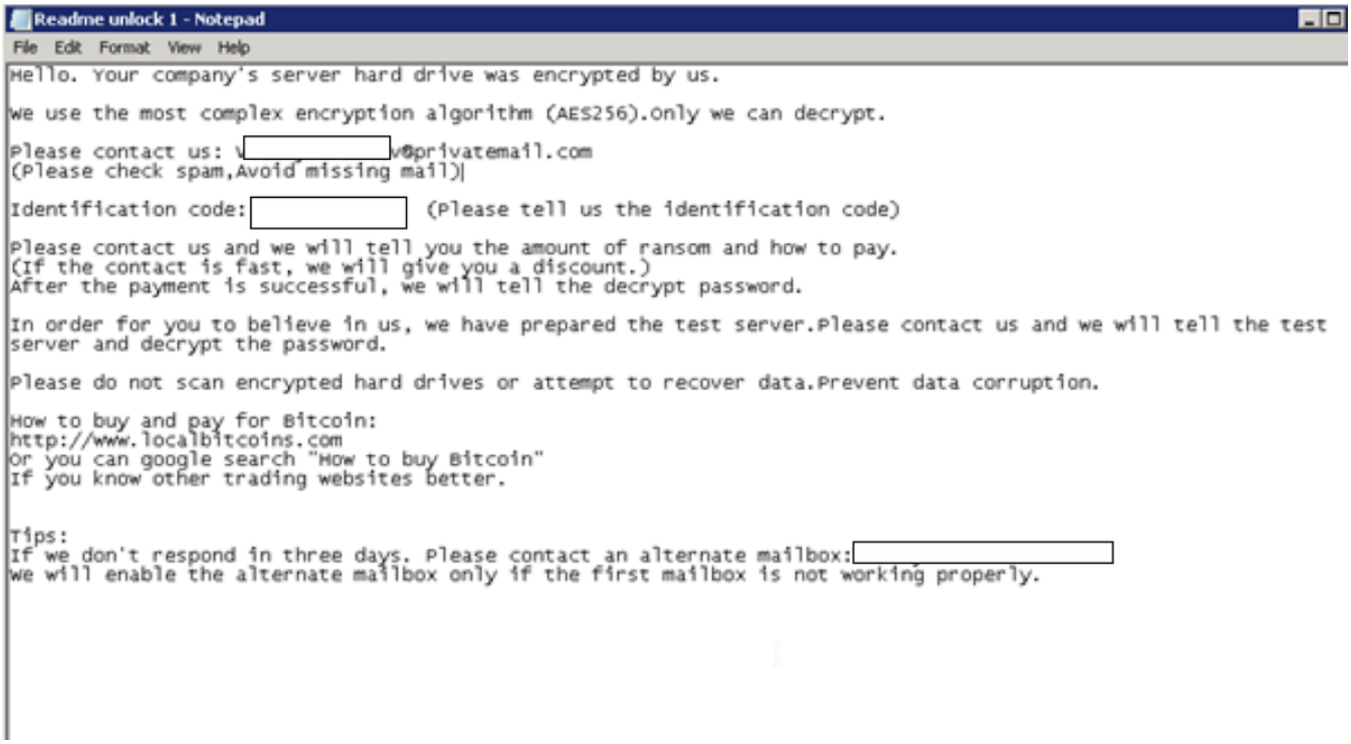
Dtrackを使った組織侵入型ランサムインシデントの分析 - セキュリティ研究センターブログ

blog.macnica.net/blog/2020/11/dtrack.html



竹内 寛

2020年11月27日 17:44

Dtrackを使った組織侵入型ランサムインシデントの分析

- APT
- インテリジェンス

- B!
- ツイート

パソコン等の端末やサーバ上のデータの暗号化等を行い、それらを復旧する事を引き換えに金銭を要求するランサムウェア攻撃。従来のメール経由でマルウェアに感染させる手口に加え、VPN等のネットワーク機器やインターネットからアクセス可能な管理サーバから企業ネットワークに侵入し内部システムを把握した後に重要サーバを使用不可にする手口も多く観測されています。これにより金銭搾取を目的とし脅迫を行うランサム攻撃は、企業にとって更に深刻なものになっています。

本記事では、弊社が過去対応を行った国内企業の海外拠点でネットワークに侵入された後に基幹システムサーバのデータ暗号化・金銭を要求されたインシデントの分析結果について共有し、対策の検討に活用していただく事を目指し記載しています。

インシデント概要

インシデント対応は、3月上旬に基幹システムのサーバにリモートアクセスできない事象が発覚した事から始まりました。調べた所、サーバのデスクトップ上に脅迫内容が記載されたファイルが見つかり、数十台のサーバでシステムドライブを除いた全ボリュームが暗号化された事が分かりました。更にデータのバックアップも暗号化されていました。

図1. 攻撃者が残した脅迫文

脅迫文の文面は、公開情報によると2018年頃に観測されたTimisoaraHackerTeam (THT) Ransomwareと呼ばれている攻撃者グループによる活動で使われた文面と一致していました。攻撃者グループの要求額は、数千万円相当のビットコインでした。

ここからは、侵入・内部活動・脅迫の各フェーズで使われた攻撃者のTTPs(Tactics, Techniques and Procedures)について解説をします。

侵入

インターネットからアクセス可能であるZoho ManageEngine Desktop Centralサーバに内在していた脆弱性 CVE-2020-10189が悪用されました。この脆弱性によりサーバに2つのファイルが設置、実行されました。

- install.bat
- storesyncsvc.dll

install.batは、storesyncsvc.dllをサービス登録するバッチファイルで、 storesyncsvc.dllは、メモリ上に商用ペネトレーションツールのCobalt StrikeのRAT Beaconを動作させるものでした。

図2. install.bat

Cobalt Strikeで遠隔操作を可能とするコンポーネントは2種類の形態があります。１つは、StagerでRAT機能を持つコンポーネント"beacon"をTeam Serverからダウンロードしてメモリ上で実行します。

図3. Stager

もう１つの形態は、Stageless で、ファイルに内部に暗号化されたbeaconのコードが埋め込まれており、実行時にメモリ上にbeaconが展開されます。

図4. Stageless

この段階で設置されたものはStagelessの形態でした。以下がbeaconの設定情報(コンフィグ)です。

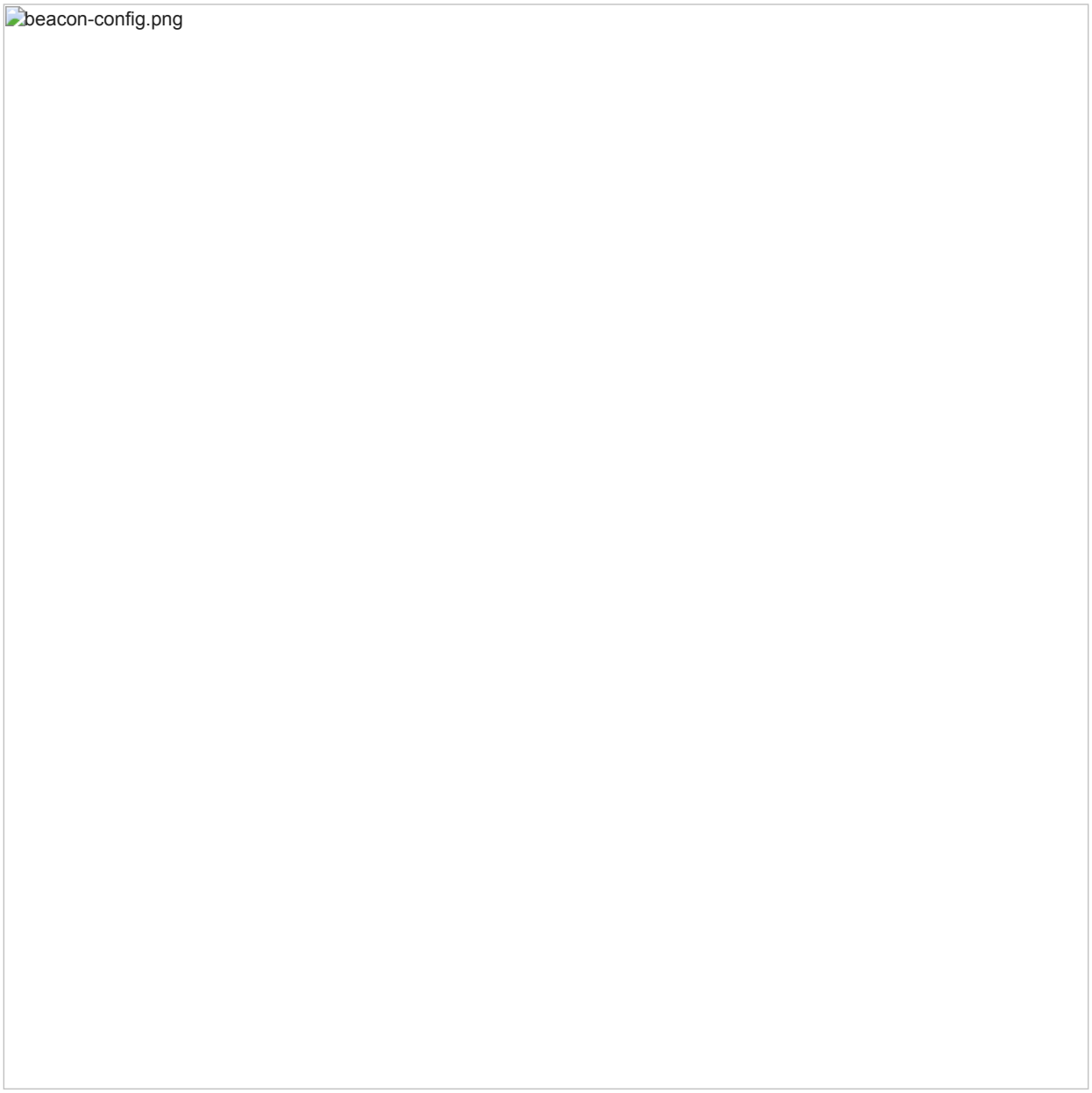


図5. storesyncsvc.dll(beacon) コンフィグ

このbeaconは、Cobalt StrikeのTeam Server(C2サーバ)とのHTTPS通信を本来のTeam Server (exchange.dumb1[.]com)ではなく、cdn.bootcss[.]com宛の通信に偽装する設定になっていました。Cobalt Strikeは、Team Serverとの通信を容易に偽装できるMalleable C2 Profile機能を有しています。

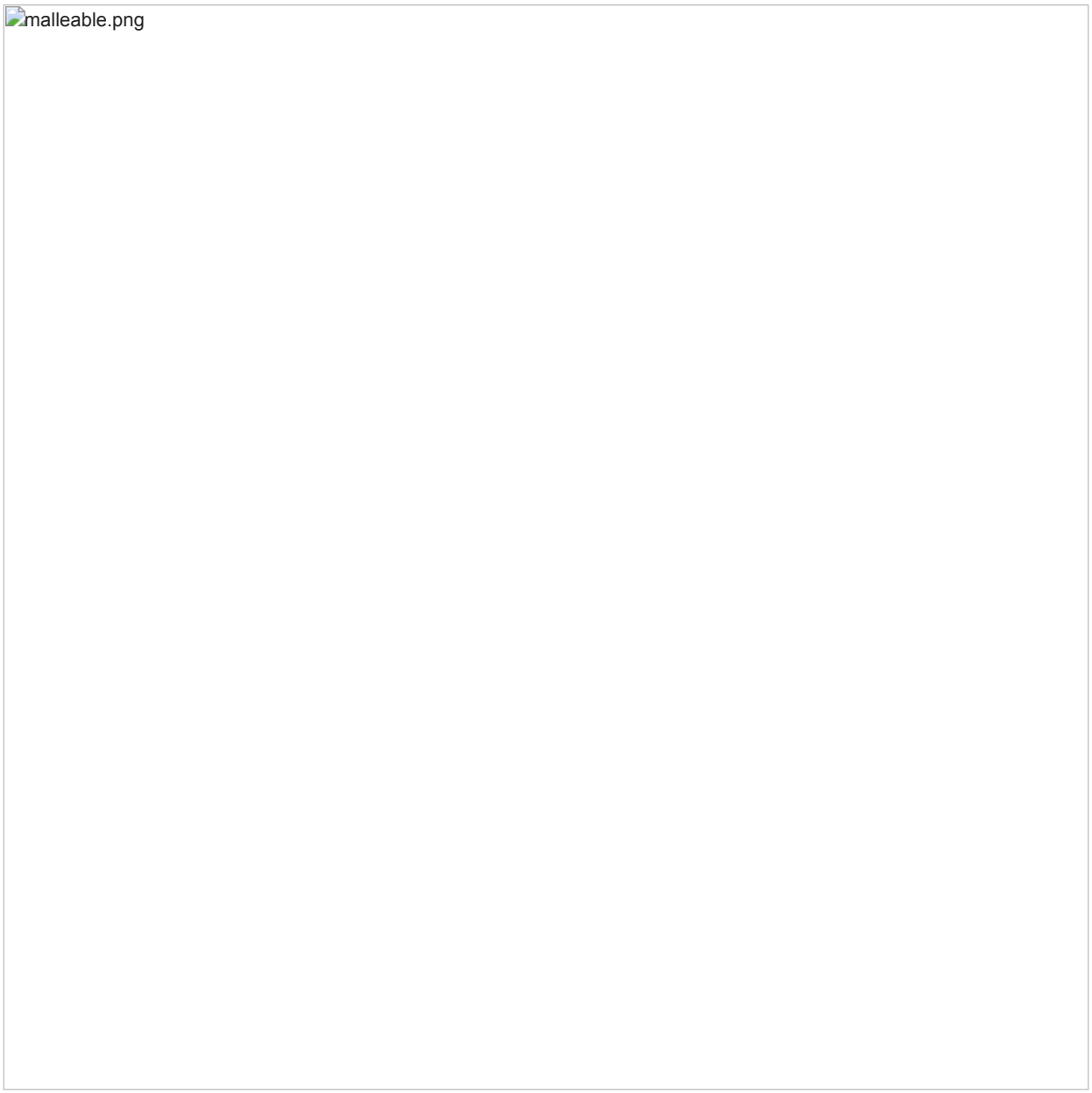


図6. Malleable C2 Profileで偽装された通信

これにより、攻撃者は最初の足場固めに成功しました。

内部活動

Zoho ManageEngine Desktop Centralサーバ上に足場固めをした後に、攻撃者は、新たなCobalt Strike Stagerをダウンロードしました。このStagerは、商用パッカーのVMProtectでパックされていました。

ここまで読まれた方の中には、気づいた方もいらっしゃるかもしれませんが、これまで解説した手口は、FireEye社のブログで解説されているAPT41/Winnti Groupの攻撃キャンペーンの手口と同一のものです。我々がインシデント対応をしている時に記事が公開され、この記事を読み本インシデントもATP41による可能性が高いと考えました。

FireEye 解析記事: This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits

APT41 + Dtrack = ?

しかし、調査を進めていく中で同じサーバ上に別のマルウェアが、Windowsの機能の１つであるBITS(Background Intelligent Transfer Service)でダウンロードされていたのを発見しました。ファイル名はmsupdate.exeで、解析の結果、Lazarusが使うRemote Administration Tool (RAT) の１つ であるDtrackである事が分かりました。

msupdate.exe の内部に暗号化されたDtrackが埋め込まれており、実行時にメモリ上に展開されます。埋め込まれている文字列の大部分がRC4で暗号化されています。実装されているC2コマンドは、Kaspersky社の解析内容とほぼ一致していました。

Kaspersky 解析記事: Hello! My name is Dtrack

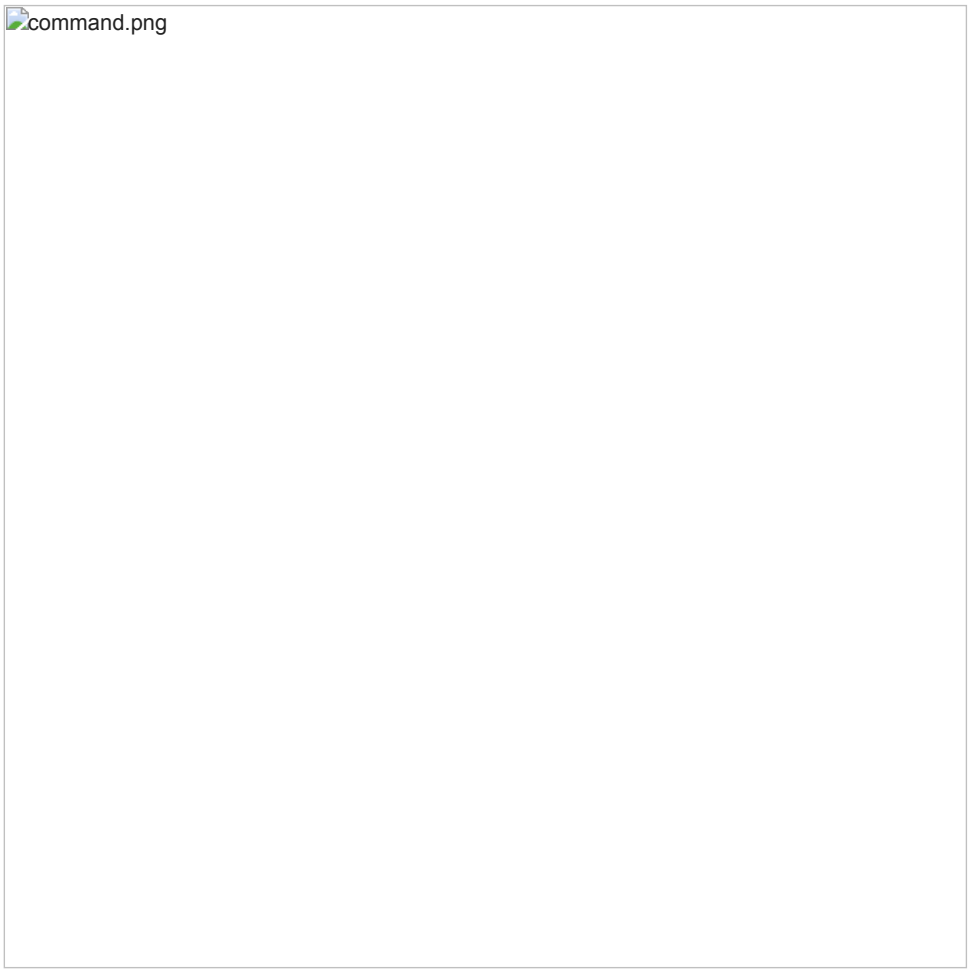


図7. Dtrack C2コマンド受信処理部分

表1. Dtrackコマンド一覧

コマンドID	命令
1003	感染機器へファイルアップロード
1005	感染機器情報をC2サーバへアップロード
1006	C2サーバへファイルダウンロード
1007	全ディスクボリュームデータをC2サーバへアップロード
1008	指定ディスクボリュームデータをC2サーバへアップロード
1018	コマンドチェックインターバル値の更新
1023	自身をアンインストール
上記以外	任意コマンドの実行

以下スクリプトは、文字列を復号するIDAPython スクリプト(Python3)です。

```
def rc4_init(key):
    index1 = index2 = 0
    box = bytearray(range(256))
    for i in range(256):
        index2 = (key[index1] + box[i]+ index2) & 0xFF
        box[i], box[index2] = box[index2], box[i]
        index1 += 1
        if(index1 == len(key)):
            index1 = 0
    return box

def rc4_crypt(buffer, box):
    x = y = 0
    for i in range(len(buffer)):
        x = (x+1)&0xFF
        y = (box[x] + y) & 0xFF
        box[x], box[y] = box[y], box[x]
        buffer[i] ^= box[(box[x] + box[y]) & 0xFF]
    return bytes(buffer)

def rc4(buffer,key):
    S = rc4_init(key)
    out = rc4_crypt(buffer,S)
    return out

enc = get_bytes(here() + 2, get_wide_word(here()), 0)
key = b"\x66\x6D\x35\x68\x6B\x62\x66\x78\x79\x68\x64\x34"

buffer = bytearray(enc)
dec = rc4(buffer, key)
print(dec)
set_cmt(here(), dec.decode('utf-8'), 1)
```

図8. RC4で暗号化された文字列

Dtrackが発見された事により、攻撃の主体がAPT41ではなくLazarusである可能性も考える必要が出てきました。

その後に攻撃者はドメイン管理者アカウント権限を奪取しました。調査からは、攻撃者がどのように権限を奪取したかを特定する事はできませんでした。攻撃者は、ドメイン管理者アカウントを不正利用し、RDP(リモートデスクトップ)を使い他サーバへの侵入を拡大させていきました。

感染拡大の中で数台のサーバにPowerShellスクリプトのStagerをサービス登録していき、その中にはドメインコントローラも含まれていました。PowerShellで実行されるコマンドは、Base64、GZIP、XOR を使い暗号化されています。

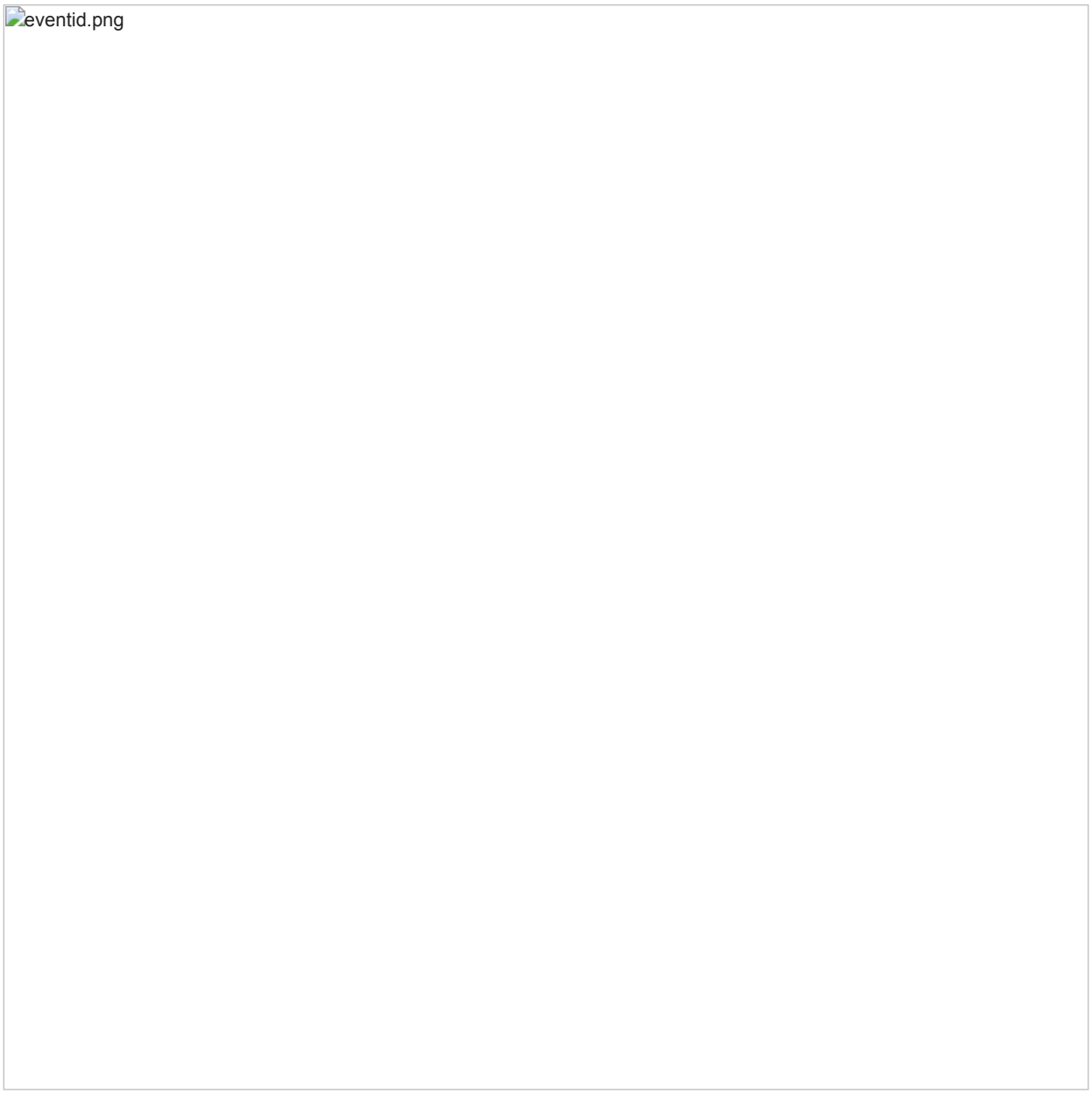


図9. Stagerを起動するサービスがインストールされた際のイベントログ

掌握したドメインコントローラを起点に、更に数十台のサーバへ活動範囲を広げていきます。

脅迫

攻撃者は、正規ツールであるJetico BestCryptを使い、サーバのディスクをボリューム単位で暗号化し、脅迫メッセージのファイルを残していきました。この手口は、公開情報にあるTHT Ransomwareと全く同一です。侵入からこの脅迫に至るまでの期間は、5日間でした。

本インシデントで分かった攻撃者のTTPをまとめると以下の通りです。

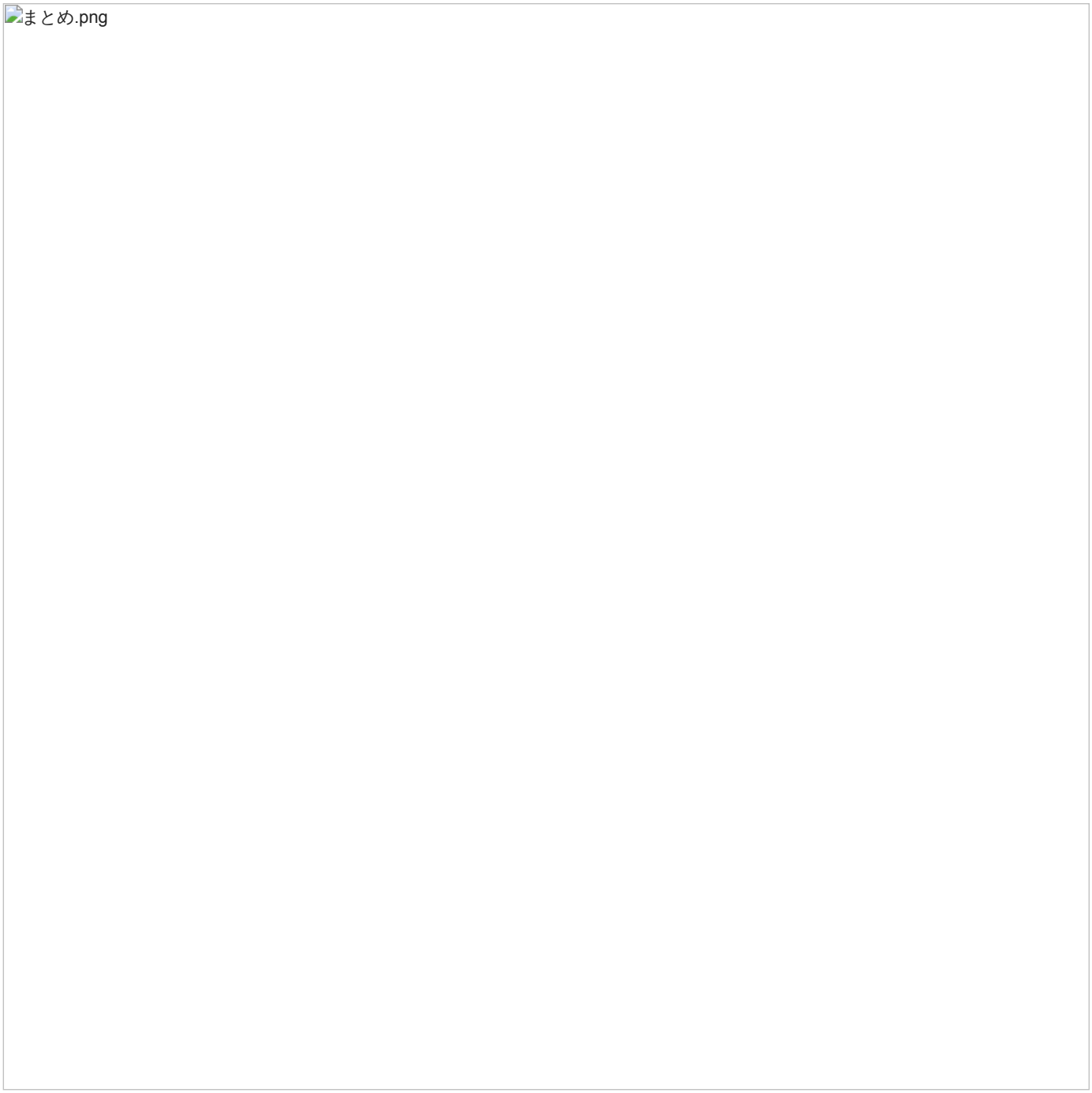


図10. 各フェーズで使われた攻撃テクニック

総括

今回のインシデント対応からの気づきとして以下が挙げられます。

侵入された後の早期検出

今回悪用された脆弱性も修正パッチリリース日とほぼ同時期に悪用され侵入をされています。侵入対策、早期のクリティカルパッチ適用は重要ですが、万が一侵入された場合に攻撃者が目的を達成する前に早期に見つける事が可能であるかを確認しておく事も重要であると考えられます。

Cobalt Strikeが発見された場合の対応

Cobalt Strikeの機能が充実している事からも、攻撃者に悪用されるケースは続く傾向にあると考えています。

上述の通り、Team Serverとの通信偽装を容易にするMalleable C2 Profile機能があるため、Cobalt Strikeが発見された場合は、可能であれば内部もしくは外部の専門家に解析を依頼しコンフィグを確認し対応に活用するのが望ましいと考えられます。セキュリティベンダーSentinel-Oneからは、コンフィグを抽出するツールが公開されています。

CobaltStrikeParser

コンフィグにあるUser-Agent が、組織内で使われていないものであれば、それもインディケータとして活用する事ができます。

足場固め後の正規ツールの悪用(マルウェアを使わない)

今回のインシデントでは、最初の足場固めと内部活動時の数台のサーバを除けば暗号化を含めマルウェアは使われていません。最初に侵入したネットワーク以降の活動ではマルウェアではなく侵害した機器にあるものや外部から正規ツールをアップロードし目的を達成する傾向が見られます。その為、マルウェア検知だけではなくエンドポイント、ネットワーク、ログベースで正常時の基準から外れたアノマリな活動を検知するしくみを検討する事も重要と考えられます。

攻撃者の帰属という観点では、なぜDtrackが使われたのかという点については、APT41とLazarusの間でツールの共有等の連携している可能性が考えられますが、現状では憶測の域を出ていません。

インディケータ情報

ファイル名	SHA256	備考
install.bat	de9ef08a148305963accb8a64eb22117916aa42ab0eddf60ccb8850468a194fc	storesyncsvc.dllをサービス登録
storesyncsvc.dll	f91f2a7e1944734371562f18b066f193605e07223aab90bd1e8925e23bbeaa1c	Cobalt Strike beacon
msupdate.exe	85d8822ea120dc87321400d03b527ce14fc308abec3da2d9e6ddff77a810319d	Dtrack
WindowsUpdate.exe	b72c2c98b4679c05706a07e069d75fb2a07a95c5c9009bb953a4ee414fa56e15	Cobalt Strike Stager (VMProtected)
bcfmgr.exe	859f845ee7c741f34ce8bd53d0fe806eccc2395fc413077605fae3db822094b4	正規暗号化ツール BestCrypt

通信先	備考
http[:]//66.42.98[.]220:12345/test/install.bat	install.bat ダウンロード元URL
http[:]//66.42.98[.]220:12345/test/storesyncsvc.dll	Cobalt Striek beacon ダウンロード元URL
https[:]//mail.gietriangle[.]org/public/src3.png	Dtrack ダウンロード元URL
http[:]//91.208.184[.]78/2.exe	Cobalt Strike Stager ダウンロード元URL
exchange.dumb1[.]com	storesyncsvc.dll の通信先
http[:]//ussainc[.]org/includes/database/mysql/libssh.php	msupdate.exeの通信先
http[:]//www.tastygoodness[.]net/modules/dashboard/dashboard.module.php	msupdate.exeの通信先
http[:]//176.123.3[.]108/9ioK	WindowsUpdate.exeの通信先
http[:]//176.123.3.108/px3A	PowerShell Stagerの通信先

この記事の筆者

竹内 寛

リバースエンジニアリング（マルウェア解析）を担当。彼の手に渡ったマルウェアはまさに“まな板の上の鯉”と同じ。あとは解析されるがまま。最近の楽しみは、ハイボールを片手に海外ドラマを鑑賞するか、マントノン侯爵夫人に会うこと。好きなマシン語は、EB FE。

前へ

Flare-On 7 Challenge Writeup

次へ

vCenter Serverの脆弱性まとめとSHODANでの観測状況