サイバーセキュリティレポート

2022.06

NTT セキュリティ・ジャパン株式会社
コンサルティングサービス部　脅威インテリジェンス管理チーム

目次

【当レポートについて】

当レポートでは 2022 年 6 月中に生じた様々な情報セキュリティに関する事件、事象、またそれらを取り巻く環境の変化の中から特に重要と考えられるトピック 3 点を選び、まとめたものである。各トピックの要旨は以下のとおりである。

第 1 章『マイクロソフト社、6 月の月例パッチでゼロデイ脆弱性「Follina」に対処』

- 米マイクロソフト社は 6 月 14 日、月例セキュリティ更新「パッチチューズデイ」にて、脆弱性「CVE-2022-30190」(通称：Follina)に対処した。
- Office のマクロが無効にされていても感染したり、リッチテキストファイルではファイルを開かずプレビューするだけで感染したりするなど、従来の対策を巧妙にすり抜ける危険な脆弱性である。
- ランサムウェア攻撃の入り口にもなる標的型攻撃メールの殆どは既知の脆弱性を狙ってくるため、この機会に端末のセキュリティアップデートが確実に行われていることを再確認することを勧める。

第 2 章『RSOCKS ボットネット、解体される』

- プロキシサービス業者「RSOCKS」のボットネットが、FBI 等、欧米の法執行機関の協働により解体された。RSOCKS を構築したのは 20 年近くサイバー犯罪に携わってきたロシア人管理者であり、Web ストアを設けて RSOCKS のサービスを提供していた。
- RSOCKS の Web ストアでは多数のプロキシサーバーを借りられるようになっていた。ショッピングサイトで、限定商品を数多く、また素早く買い占めようとする転売業者や、リスト型攻撃を行うサイバー犯罪者が、RSOCKS のサービスを利用していたとみられている。
- RSOCKS は解体されたものの、今後もボットネットによるプロキシサービスが現れ、転売業者やサイバー犯罪者が利用することが予想される。今後も Web セキュリティでは IP アドレスベースのみに頼らない対策が必要である。

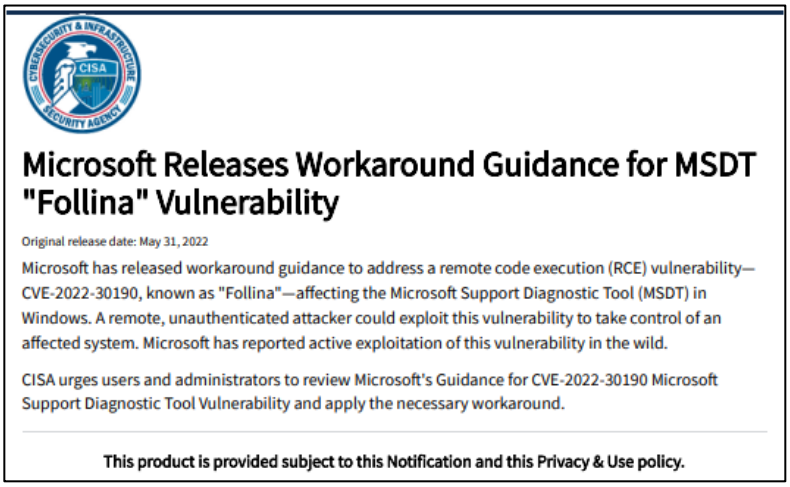
第 3 章『RDP へのブルートフォース攻撃』

- 図書館の受託運営等を手掛けるヴィアックス社が、外部に公開していたリモートデスクトップ接続がブルートフォース攻撃によってハッキングされ、自社ネットワーク内でランサムウェア感染被害が発生したことを発表した。
- 攻撃者はダークウェブでブルートフォース攻撃用ツールを入手し、ターゲット組織のシステムに侵入するだけでなく、RDP のアカウントとパスワードを RDP shop と呼ばれる闇市場で販売する。
- コロナ渦のリモートワークによって、RDP へのブルートフォース攻撃が増加したとの分析がある。ブルートフォース攻撃には長く複雑なパスワードや多要素認証が有効であるが、さらにファイアウォール等を利用してリモートデスクトップ接続元 IP アドレスを制限するか、社員に VPN 経由で RDP を使用させることを推奨する。

1. マイクロソフト社、6 月の月例パッチでゼロデイ脆弱性「Follina」に対処

1.1. 概要

米マイクロソフト社は 6 月 14 日、月例セキュリティ更新「パッチチューズデイ」にて、脆弱性「CVE-2022-30190」(通称：**Follina**)に対処した[1]。この脆弱性は「Microsoft Support Diagnostic Tool (MSDT)」に関するもので、Office のマクロが無効化されていても任意の PowerShell コマンドを実行することができる。パッチに先立ち 5 月末にマイクロソフトが回避策を提示した際には、米国の CISA も対応を推奨するアドバイザリをリリースするなど高い注目を集めていた。この脆弱性をセキュリティ研究者が公開した時点で、既に当脆弱性を利用した攻撃が確認されており、約半月後にパッチが提供されるまで「ゼロデイ脆弱性」であった。



Microsoft Releases Workaround Guidance for MSDT "Follina" Vulnerability

Original release date: May 31, 2022

Microsoft has released workaround guidance to address a remote code execution (RCE) vulnerability—CVE-2022-30190, known as "Follina"—affecting the Microsoft Support Diagnostic Tool (MSDT) in Windows. A remote, unauthenticated attacker could exploit this vulnerability to take control of an affected system. Microsoft has reported active exploitation of this vulnerability in the wild.

CISA urges users and administrators to review Microsoft's Guidance for CVE-2022-30190 Microsoft Support Diagnostic Tool Vulnerability and apply the necessary workaround.

This product is provided subject to this Notification and this Privacy & Use policy.

図 1 CISA による Follina の回避策適用を推奨するアドバイザリ[2]

1.2. 脆弱性 Follina について

【Microsoft Support Diagnostic Tool (MSDT) とは】

Follina が見つかった MSDT は Windows に標準搭載されているサポート診断ツールである。マイクロソフトの製品ごとに本ツールのパッケージが用意されており、それぞれの製品でのトラブルシューティングに必要なログ収集が行われる。マイクロソフトの説明によると、本ツールには「自動スクリプトの一部としてトラブルシューティングパックを呼び出し、ユーザー入力なしで追加のオプションを有効にする」[3]機能がある。このファイルに埋め込んだスクリプト経由で MSDT を呼び出すことができるという特徴が、Follina で悪用されている [6]。

---

[1] 出典：Microsoft Security Response Center『2022 年 6 月のセキュリティ更新プログラム (月例)』
https://msrc-blog.microsoft.com/2022/06/14/202206-security-updates/

[2] 出典：CISA『Microsoft Releases Workaround Guidance for MSDT "Follina" Vulnerability』
https://www.cisa.gov/uscert/ncas/current-activity/2022/05/31/microsoft-releases-workaround-guidance-msdt-follina-vulnerability

[3] 出典：Microsoft『msdt』
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/msdt

【Follina 発見から命名の経緯】

問題が表面化したきっかけは、ベラルーシの IP アドレスから、Google が提供するオンラインウイルススキャンサービス「VirusTotal」にアップロードされた奇妙な Word 文書ファイルであった。5 月 27 日、日本のサイバーセキュリティ研究者「nao_sec」がこれを発見した[4]。

図 2 Follina を発見した nao_sec のツイート[5]

この文書ファイルは、文書内で使用するテンプレートを外部からダウンロードする Word の機能を利用して HTML ファイルをダウンロードさせ、さらにその HTML ファイル経由で MSDT を呼び出すことで、任意のコマンドを実行できるようになっていた。本来このような挙動はブロックされるべきだが、マイクロソフトのウイルス防衛機能「Defender for Endpoint」はこれをブロックしなかった[6]。

この脆弱性が特に危険な点として、マクロが無効になっていても防ぐことができないこと、Word 形式だけでなく RTF 形式(リッチテキスト)のファイルにも埋め込みが可能であること、さらに RTF 形式の場合、ファイルを開かずプレビューするだけでコードが実行されること等が挙げられる。

この文書ファイルは「05-2022-**0438**.doc」という名前であり、「0438」はイタリアの都市フォッリーナの市外局番であった。このことにちなみ、別のセキュリティ研究者 Kevin Beaumont 氏が当該脆弱性を「Follina」と名付けた[6]。

---

[4] 出典：トレンドマイクロセキュリティブログ『Microsoft 製品のゼロデイ脆弱性「Follina（CVE-2022-30190）」が発見される』
https://blog.trendmicro.co.jp/archives/31412

[5] 出典：Twitter『@nao_sec』
https://twitter.com/nao_sec/status/1530196847679401984

[6] 出典：DoublePulsar『Follina — a Microsoft Office code execution vulnerability』
https://doublepulsar.com/follina-a-microsoft-office-code-execution-vulnerability-1a47fce5629e

1.3. Follina 発見前のセキュリティ状況

マイクロソフトは猛威を振るい続けていたマルウェア「Emotet」等、Office のマクロを利用したマルウェアへの対策として、今年 4 月より、インターネットからダウンロードされたファイルについては Office のマクロをデフォルトで無効にするという変更を行った。マイクロソフトのサイバー犯罪インテリジェンスリーダーである Nick Carr 氏は、この変更を「セキュリティにおいて、データに基づく意思決定は他の多くのビジネス原動力に勝る」「大きな進歩だ」と述べていた[7,8](ただしマイクロソフトは 7 月上旬にはこの変更を一旦撤回。再リリースについては未定である[9])。

この「進歩」から 1 か月ほどで、ファイルを開くだけ、条件によってはプレビューするだけで感染する脆弱性がみつかったことや、既に攻撃に利用されているというショックから、Follina は大きく取り上げられることになった。

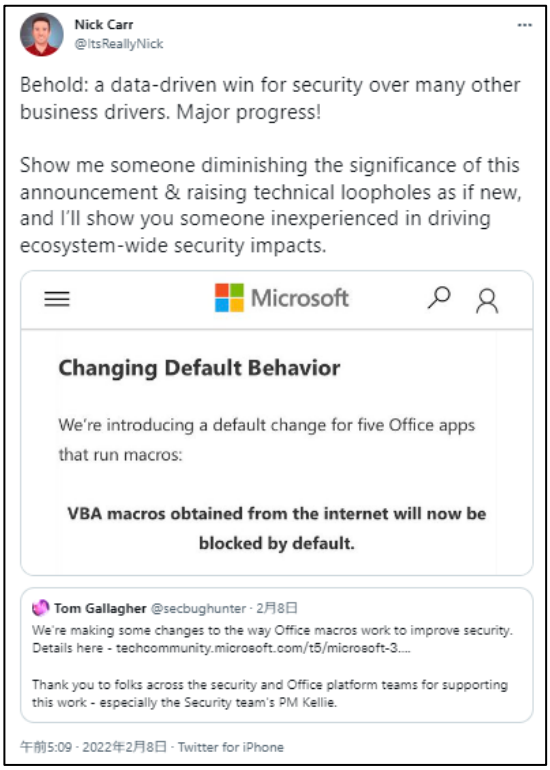


図 3 Nick Carr 氏のツイート

1.4. これまでに観測されている Follina を利用した攻撃

Follina を命名した Kevin Beaumont 氏のブログによると、「nao_sec」による発見の 1 か月前の 2022 年 4 月には既に、Follina を悪用した Word ファイルが VirusTotal にアップロードされていた。その文書はロシア語で書かれており、ロシアのメディアであるスプートニクラジオのインタビューへの招待を装った内容であった。また、セキュリティ会社 Proofpoint によると欧州

[7] 出典：Twitter『@ItsReallyNick』
https://twitter.com/ItsReallyNick/status/1490779702046433292
[8] 出典：TechTarget『Microsoft disables VBA macros by default』
https://www.techtarget.com/searchsecurity/news/252513141/Microsoft-disables-VBA-macros-by-default
[9] 出典：ZDNet『MS、「Office」での VBA マクロブロック機能を無効化』
https://japan.zdnet.com/article/35190239/

政府や米地方自治体を標的とした攻撃も確認されている[10]。さらに、中国の国家利益に関与しているとみられる APT グループ「TA413 CN」もチベット亡命政府の「女性支援デスク」になりすまし、Follina を利用した Word ファイルを配布していることが観測されている [10]。

このように攻撃者も攻撃対象も多様であり、Follina が国家を背景とした攻撃グループによって、すでに幅広く利用されている状況であることがうかがえる。

1.5. まとめ

これまで Office 形式を狙った代表的なマルウェアは Emotet であり、マクロを実行させることでマルウェア感染を狙っていた。Emotet が 2014 年に初めて観測されて以来、国内外のセキュリティ機関から再三注意喚起が出されてきたが、今年に至っては感染が再拡大している状況である[11]。マクロが無効でも攻撃可能な Follina は、攻撃者にとって新しい強力な武器となり、今後、長期に渡って悪用される可能性が高い[12]。

ランサムウェア攻撃の入り口にもなる標的型攻撃メールの殆どは既知の脆弱性を狙ってくるため、この機会に端末のセキュリティアップデートが確実に行われていることを再確認してはいかがだろうか。

[10] 出典：Bleeping Computer『Windows zero-day exploited in US local govt phishing attacks』
https://www.bleepingcomputer.com/news/security/windows-zero-day-exploited-in-us-local-govt-phishing-attacks/

[11] 出典：JPCERT/CC『マルウェア Emotet の感染再拡大に関する注意喚起』
https://www.jpcert.or.jp/at/2022/at220006.html

[12] 出典：TECH＋『Office の脆弱性が中国の犯罪グループに悪用されている、警戒を』
https://news.mynavi.jp/techplus/article/20220602-2357194/

2. RSOCKS ボットネット、解体される

2.1. 概要 [13]

2022 年 6 月 16 日、米国の司法省はドイツ、オランダ、英国の法執行機関と共にロシアのプロキシサービス業者「RSOCKS」のボットネットを無効化したことを発表した。捜査から、RSOCKS が提供していたプロキシサーバーが、家庭にあるハッキングされた機器（IoT、Android 機器、パソコン）から成るボットネットであったことが判明した。RSOCKS のサービスは主に転売業者によるネットショップの限定商品の買い占めのほか、サイバー犯罪者によるリスト型攻撃といった不正アクセスにも使用されていたとみられている。

RSOCKS の運営者は、長年ハッキングに関わってきたロシア人であり、サービス提供のために会社を運営していたことが判明している。

2.2. プロキシサービス業者へのニーズの背景

【転売事業者の存在】[14]

ナイキ等スニーカーのメーカーは、例えばジョーダンモデルといった限定版モデルをたびたび発売している。転売業者らはこのような商品の買い占めを行い、フリーマーケットサイト等でマニアに高く転売することで、大きな差益を得ようとする。このため、消費者がスニーカーを定価で買えない事態が頻発し、問題視されている。

ショッピングサイトでは 1 人あたりの購入数を制限しているが、転売業者は制限を超えて購入する目的で、複数のアカウントを取得して買い漁る。さらに、購入は早い者勝ちなので、ショッピングサイトでの購入処理を自動・高速化したプログラム（ボット）を活用して、人間が買うよりも素早く購入する。このようなツールは、限定版スニーカーの転売業者が使ったことからスニーカーボットと呼ばれ、現在、スニーカーのショッピングサイトに限らずさまざまなショッピングサイトで、転売業者が利用している[15]。

【プロキシサービス業者へのニーズ】

ショッピングサイトでは転売目的の購入や複数のアカウントの取得を約款で禁じているが、それだけでは実効性が無いため、不正の兆候があるとアクセスを制限する対策を、サーバー側で施している。例えば、特定の IP アドレスから複数のアカウントにログインがあると、制限以上の購入を意図しているとみなして接続を拒否する。また、過去に不正行為のあった IP アドレスや不正行為の多い特定国の IP アドレスを集めたブラックリストでブロックを行い、不正を予防しようとしている。

一方、転売業者もアクセス元を隠すことで対抗する。その際に使われるのが転売業者の IP アドレスとショッピングサイトの間に入り、転売業者の代理でアクセスするプロキシサーバーである。プロキシサーバーはひとつひとつ IP アドレスが異なるため、複数のプロキシサーバーを用意してアカウントごとに使えば、接続拒否されない。また、プロキシサーバーの IP アドレスがブラックリストに入っても、使い捨ててまた別のプロキシサーバーで接続すればブラックリストを回避できる。この方法には大量のプロキシサーバ

[13] 出典：マイナビ TECH+『数百万台をハッキングしたロシアのボットネット RSOCKS を解体、米司法省ら』
https://news.mynavi.jp/techplus/article/20220620-2372478/

[14] 出典：GQ『The War Against Sneaker Bots Peaked at the End of 2018』
https://www.gq.com/story/war-against-sneaker-bots

[15] 出典：ITmedia NEWS『1 日に 1.15 億回以上 急増する不正ログインの裏に“bot の存在”：迷惑 bot 事件簿』
https://www.itmedia.co.jp/news/articles/1904/19/news008.html

ーが必要になるので、転売業者はプロキシサーバーを何百万と所有しているプロキシサービス業者から借りて使用している。
転売業者以外にも、大量に作成した偽アカウントによる SNS や動画サイトでの「いいね！」の操作等、不正な行為のインフラ提供者としてプロキシサービスは利用されている。

2.3. RSOCKS のサービス提供

【高評価のプロキシサービス業者、RSOCKS】

RSOCKS は 2014 年頃から誰でもアクセスすることができるインターネット上に Web ストアを設け、多数のプロキシサーバーのアクセス権を販売していた。IP ブラックリストに載りにくい**住宅用 IP アドレスに偽装できる**ため評価が高く、プロキシサービス業者の評価サイトが実施したテストでは、RSOCKS の提供する IP アドレスの約 76%がブロックされずに、Amazon 等のサイトへのアクセスに成功していた。

【RSOCKS の料金プラン】

RSOCKS のアクセス権の料金プランは IP アドレスの量と時間制（日／週／月）で決められていて、契約時間内であれば転送データ量に関係なく使い放題であった。スニーカーボット向けのプロキシサービス業者の中では標準的かやや高めな料金設定で、例えば 1 日利用した場合、2,000 IP アドレスで$30 を、90,000 IP アドレスで$200 を請求していた。料金プランは 20 パターン以上あり、動画サイトといった特定の Web サービスへのアクセス向けにカスタマイズしたプランも用意していた。評価サイトでは、他の同類のサービスよりプランが多く、使い方に合わせて柔軟に選べると評価されていた。
顧客サポートも行き届いており、FAQ ページのほか迅速に対応するメール/ライブチャットでのサポートを備えていた。

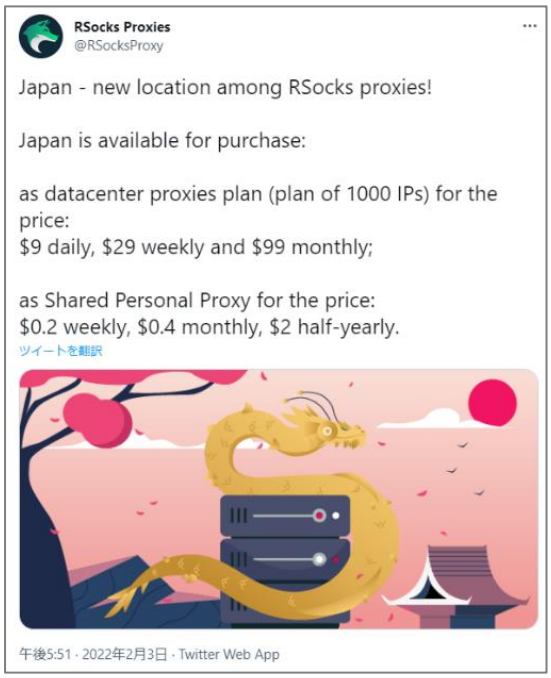


図 4　日本の IP アドレスのプロキシ提供を発表する RSOCKS 公式のツイート [16]

【住宅用 IP アドレスの正体】 [17]

捜査に当たった FBI が、身元を隠してサービスを購入し分析したところ、RSOCK の正体はインターネットに繋がれた IoT デバイス（ルーター、ビデオストリーミングデバイス、スマートキー等）や、Android 機器、パソコンといった**ハッキングされた数百万のデバイスの集合体（ボットネット）**であった。
探索の結果、個人宅をはじめ大学、ホテル、スタジオ、電子機器メーカー、在宅事業者等において端末が発見された。端末の分析から、ボットネットからのブルートフォース攻撃（パスワード総当たり攻撃）で乗っ取られ、ボットネットに組み込まれたとみられている。

[16] 出典：Twitter『@RSocksProxy』
https://twitter.com/RSocksProxy/status/1489159570475864064
[17] 出典：米国司法省『Russian Botnet Disrupted in International Cyber Operation』
https://www.justice.gov/usao-sdca/pr/russian-botnet-disrupted-international-cyber-operation

【リスト型攻撃のインフラ】[18]

リスト型攻撃は、不正アクセス等で漏えいしたIDとパスワードのリストを使い、別のWebサービスに対して大量のログイン試行をすることによりアカウント乗っ取りなどを狙ったサイバー攻撃である。攻撃者は、RSOCKSのようなプロキシサービスを使うことで、接続元のIPアドレスの制限をかいくぐるだけでなく、大量のアクセス試行を検知されないようにツールを使用して接続頻度等を調整してアクセスする等、検知・遮断を困難にしている。最近も設定を緩めていたWAFが攻撃を検知できなかったという日本企業の被害報告も発表[19]されている。

米国司法省は今回の発表で、サイバー犯罪者が認証サービスに対する大規模なリスト型攻撃で、RSOCKSを利用していた可能性を指摘[20]している。

2.4. RSOCKSの運営者

【RSOCKS運営者】

セキュリティ研究者の身元調査から、RSOCKSと名乗る、現在35歳のロシア国外に住むロシア人男性が、プロキシサービスのRSOCKSの運営者と特定[21]されている。司法省の発表が身柄に言及していないことから、RSOCKSは逮捕されていないと考えられている。[22]

RSOCKSは、以前はStanxと名乗っていたことが判明している。2000年代に活動していた有力なハッキングフォーラム「RUSdot」の主要メンバーの一人であり、2010年にコミュニティが崩壊するまで所属していた。Stanxについての情報から、シベリア地方の大都市であるオムスク出身の「Denis "Neo" **Kloster**」という人物がRSOCKSであることが浮かび上がった。

【Klosterの会社】

Klosterは自身のビジネスサイトを設けていた。そこに記載された履歴によると、彼はオムスクで生まれ、12歳で初めてコンピューターに触れ、16歳で高校を卒業した。それからオムスクの大企業でシステム管理者、Web開発者、写真家としても働いてきた。最初の本格的な仕事はオンライン広告企業の立ち上げで、一時期はニューヨークに住んでいたこともある。2013年に広告業を辞め、世界を旅した後に、世界中の顧客に向けてセキュリティと匿名性のサービスの提供をうたった新会社を設立した。

---

[18] 出典：Cloudflare『クレデンシャルスタッフィングとは？』
https://www.cloudflare.com/ja-jp/learning/bots/what-is-credential-stuffing/

[19] 出典：株式会社クイック『弊社運営の看護師および看護学生向けコミュニティサイト「看護roo!」への"なりすまし"による不正アクセスについて【第3報】』
https://919.jp/wp/wp-content/uploads/2022/07/22.7.6_kangoroo_T.pdf

[20] 出典：米国司法省『Russian Botnet Disrupted in International Cyber Operation』
https://www.justice.gov/usao-sdca/pr/russian-botnet-disrupted-international-cyber-operation

[21] Krebs on Security『Meet the Administrators of the RSOCKS Proxy Botnet』
https://krebsonsecurity.com/2022/06/meet-the-administrators-of-the-rsocks-proxy-botnet/

[22] 出典：Bleeping Computer『Russian RSocks botnet disrupted after hacking millions of devices』
https://www.bleepingcomputer.com/news/security/russian-rsocks-botnet-disrupted-after-hacking-millions-of-devices/

2016 年に Kloster は、会社の運営の 3 周年を記念する記事を上記のサイトに投稿している。2016 年の 3 年前といえば、RSOCKS ボットネットのサービス開始時期と重なる。投稿によると、オムスクにある Kloster の会社には 20 数名近くの従業員がおり、集合写真（図 5）とともに「私たちは今、情報セキュリティと匿名性の分野で発展しており、世界中の何千人もの人々に使われる製品を作っている。・・・私たちはただ一緒に働くだけでなく、友達でもなく、家族なんだ」と記していた。彼ら従業員も RSOCKS のスタッフの可能性がある。

図 5 Kloster と従業員の集合写真

2.5. まとめ

プロキシサービス業者としての RSOCKS が解体された後、アンダーグラウンドコミュニティの掲示板に RSOCKS の名前で、別のサービスを再び立ち上げて戻ってくるというメッセージが残されていた[23]。プロキシサービス業者に対する転売事業者やサイバー犯罪者達のニーズは根強いと考えられる。今後も Kloster、または彼のような人物が、ボットネットを使用した同様のサービスを提供することが考えられる。

日本においてもリスト型攻撃により、サーバー側での対策をかいくぐった不正アクセスによる情報漏えい、アカウント乗っ取りによるポイント不正使用等が続いている。プロキシサービス業者を利用した攻撃を意識し、Web サイトが提供するサービス内容に応じて、多要素認証や CAPTCHA 等を導入する等、アクセス元の IP アドレスベースに留まらない対策の検討が必要である。

[23] 出典：Krebs on Security『Meet the Administrators of the RSOCKS Proxy Botnet』 https://krebsonsecurity.com/2022/06/meet-the-administrators-of-the-rsocks-proxy-botnet/

3. RDP へのブルートフォース攻撃

3.1. ヴィアックス社への攻撃[24]

2022 年 6 月 1 日、ダイレクトマーケティング事業や図書館の受託運営等を行っている株式会社ヴィアックスは、同社の勤怠・人事給与管理システムがランサムウェア攻撃を受けたことを明らかにした。この攻撃により従業員（1,872 名）、退職者（2,167 名）、扶養者、世帯主も含む計 6,800 名以上に関して、氏名、住所、支払い給与データ等が暗号化された。さらに同社は、ランサムウェアグループから身代金の要求があったと述べている。

データセンターと外部との境界（DMZ）にある勤怠システムの Web サーバーをメンテナンスする際、外部から同サーバーへのリモートデスクトップ接続が可能になっていた。これはメンテナンス設定の都合により生じた状態であったが、この機に乗じて外部からブルートフォース攻撃が実行され、リモートデスクトップ接続のパスワードが特定されてしまった。攻撃者は窃取したアカウントで当該システムに侵入した後、外部から持ち込んだランサムウェアを実行した可能性がある。

3.2. RDP へのブルートフォース攻撃について

【ヴィアックス社への攻撃に利用された RDP】[25]

Windows 環境にて、遠隔からサーバーを操作する為に利用するリモートデスクトップサービスのプロトコルを **RDP（Remote Desktop Protocol）**と呼ぶ。RDP は主に TCP 3389 番ポートを使用し[26]、外部から社内 LAN への接続に利用できるため、社内 LAN 内でランサムウェアの展開を狙う攻撃者にとって、組織に侵入する際の足掛かりの一つとして悪用されやすい。

【ブルートフォース攻撃とは】[27]

ブルートフォース攻撃は総当たり攻撃とも呼ばれ、正しいパスワードが見つかるまで、考えられるすべての英数字等の組み合わせを試す方法で、桁数が不十分なパスワードを利用していると、この攻撃により特定される恐れがある。

---

[24] 出典：ヴィアックス『勤怠管理システムサーバに対する攻撃について』
https://www.viax.co.jp/pdf/20220601.pdf

[25] 出典：MITRE『Remote Services: Remote Desktop Protocol』
https://attack.mitre.org/techniques/T1021/001/

[26] 出典：CyberArk『Explain Like I'm 5: Remote Desktop Protocol (RDP)』
https://www.cyberark.com/resources/threat-research-blog/explain-like-i-m-5-remote-desktop-protocol-rdp

[27] 出典：Kaspersky『Brute Force Attack: Definition and Examples』
https://www.kaspersky.com/resource-center/definitions/brute-force-attack

【ダークウェブでの取引】

ハッカーはブルートフォース攻撃で得たRDPの認証情報を自ら使用してターゲット組織のシステムに侵入するだけでなく、入手した認証情報をダークウェブ上のRDP shopと呼ばれる闇市場にて数ドルで販売する場合がある[28]。過去には、国際空港のセキュリティシステムへのアクセスが10ドルで提供されていたこともあった[29]。

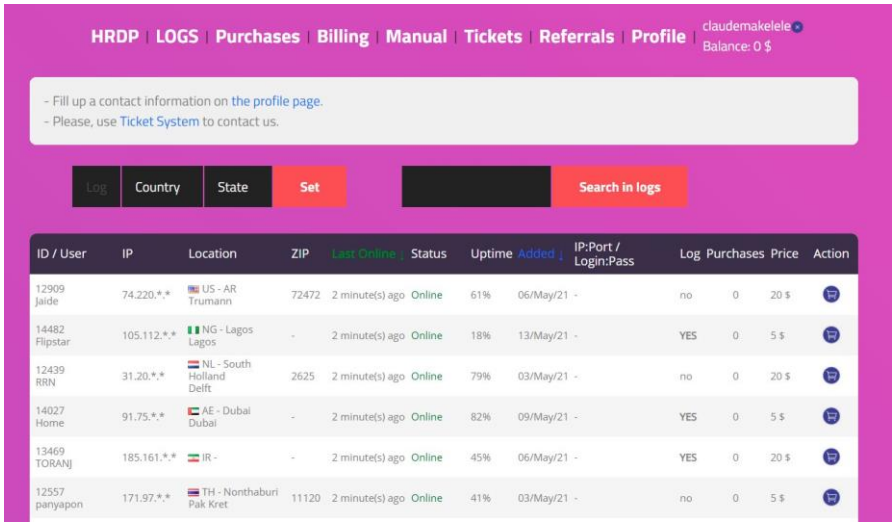


図 6 ハッキングフォーラムで宣伝されていたRDP shop

【ブルートフォース攻撃用ツール】

RDPに対するブルートフォース攻撃に使用するツールは複数、出回っている。特にHydra[30]は、ペネトレーションテストに使われるKali Linuxにプリインストールされているため、誰でも入手が可能である。ソースコードは公開されており、カスタマイズできる。また自動的に並列処理を行うため、高速で攻撃を実行する特徴がある。

類似したツールはダークウェブでも見つけることができる。 RDPの認証を狙った有用な攻撃ツールは、ハッカー掲示板を通じて攻撃者の間で広まり、多くのハッキングに利用されている。

図 7 Hydraのロゴ

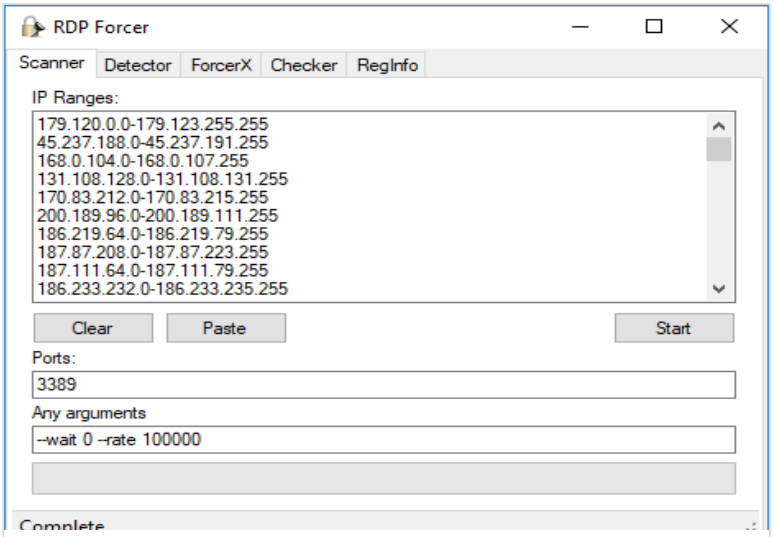


図 8 ハッカー掲示板で入手できる攻撃用ツールRDP Forcer

[28] 出典：Twitter『@campuscodi』
https://twitter.com/campuscodi/status/1395142772177448961

[29] 出典：McAfee『Major International Airport's Security System Found for Sale on Dark Web RDP Shop』
https://www.mcafee.com/blogs/internet-security/airport-security-system-dark-web-rdp-shop/

[30] 出典：Kali Linux『Hydra』
https://www.kali.org/tools/hydra/

【コロナ禍で急増する RDP へのブルートフォース攻撃】[31]

コンピューターセキュリティ会社 Kaspersky の調査によると、RDP へのブルートフォース攻撃件数は 2020 年 3 月頃に急増した後、毎月 3 億件以上という状況が続いている。コロナ渦のリモートワークの増加によって、自宅からオフィスにあるパソコンを操作する手段として、RDP を使ったリモートデスクトップ接続が急増したことが背景にあると、同社は分析している。今後も一定数の企業がテレワークを継続することが予想されるため、RDP へのブルートフォース攻撃件数は減少しない可能性が高い。

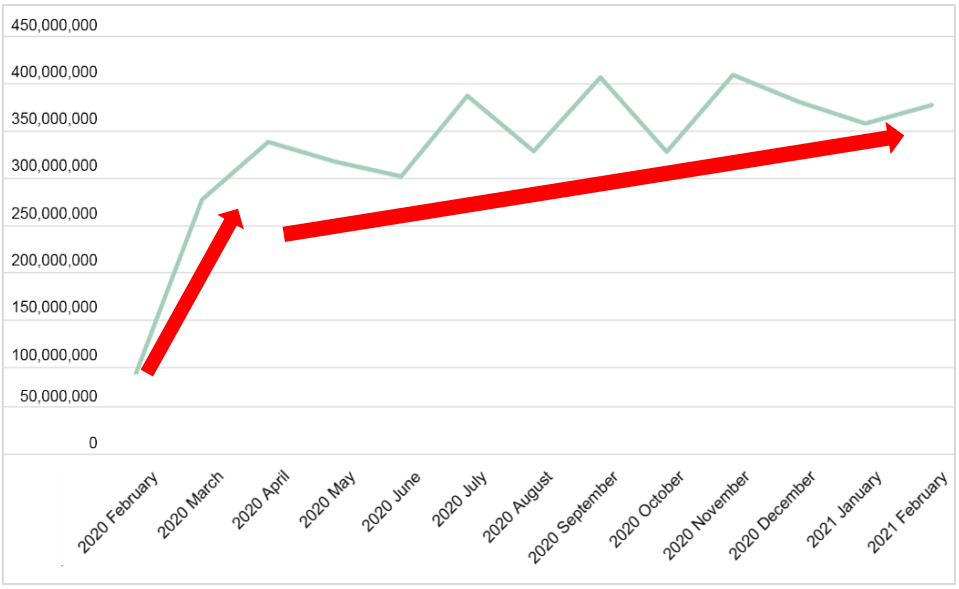


図 9 RDP に対する総当たり攻撃の総数:全世界

3.3. まとめ

急増したリモートワークに対応するため、オフィス内の端末への接続に RDP を利用することが増えており、この状況が、内部のファイルの暗号化を狙うランサムウェア攻撃者にとって、格好の侵入経路となっている。RDP へのブルートフォース攻撃には、長く複雑なパスワードや多要素認証が有効である。しかし、これらの対策を施しても、リモートデスクトップサービスの脆弱性を狙われる恐れがあるため、ファイアウォール等での接続元の制限や、RDP 接続には VPN を必須にする等、複合的な対策を推奨する[32]。

以上

[31] 出典：カスペルスキー公式ブログ『コロナ禍の 1 年：リモートデスクトッププロトコルへの攻撃が高い水準を維持』
https://blog.kaspersky.co.jp/attacks-on-rdp-during-pandemic-year/30354/

[32] 出典：サイバーセキュリティ情報局 『危険が増すリモートアクセスとパンデミックに便乗するサイバー攻撃』
https://eset-info.canon-its.jp/malware_info/special/detail/210407.html

免責事項

本記事の内容は、正確であることに最善を尽くしておりますが、内容を保証するものではなく、本記事の利用に起因して発生したいかなる損害、損失についても補償しませんのでご留意ください。記事内に誤植や内容の誤り、その他ご指摘等、お問い合わせ事項がある場合は、お手数ですが下記までご連絡ください。

お問い合わせ先：NTT セキュリティ・ジャパン株式会社

コンサルティングサービス部　脅威インテリジェンス管理チーム
メールアドレス： WA_Advisorysupport@ntt.com