商用RATのエコシステム: Unit 42、高機能商用RAT Blackremote RATの作者を公開後数日で特定

unit42.paloaltonetworks.jp/blackremote-money-money-money-a-swedish-actor-peddles-an-expensive-new-rat/

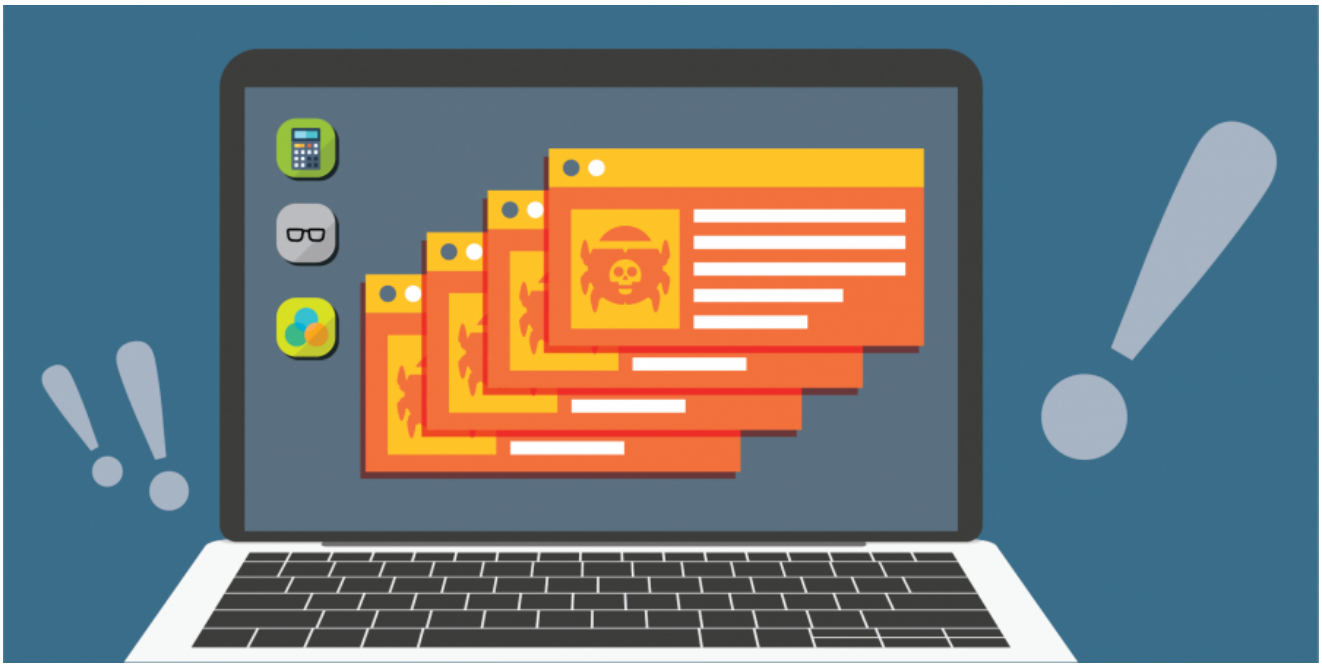
Unit 42 October 16, 2019

By Unit 42

10月 16, 2019 at 1:54 AM

Category: Malware, Unit 42

Tags: Blackremote, commodity, Cybercrime, RAT



This post is also available in: English (英語)

概要

2019年9月、Unit 42のリサーチャーによる商用リモートアクセスツール（RAT）類の調査中、これまでのところ文書化された情報がない新しいRATが発見されました。本稿ではこの新しいRATマネージャー/ビルダー、クライアント マルウェアについて報告し、背後にいるスウェーデン人開発者と同氏のマルウェア販売プロモーション方法について説明します。また、既にインターネット上で観測されている同RATを利用した攻撃に関する情報もまとめます。

RATの販売プロモーション

2019年9月の第一週、Speccy、Rafikiというハンドル名を使用するアクターが複数の地下フォーラム（図1）で新しいRATを宣伝しはじめました。宣伝用の短い投稿で彼は販売サイトblackremote[.]proへのリンクを共有しており、このとき利用されたDiscordのハンドル名はSpeccy＃0100でした。

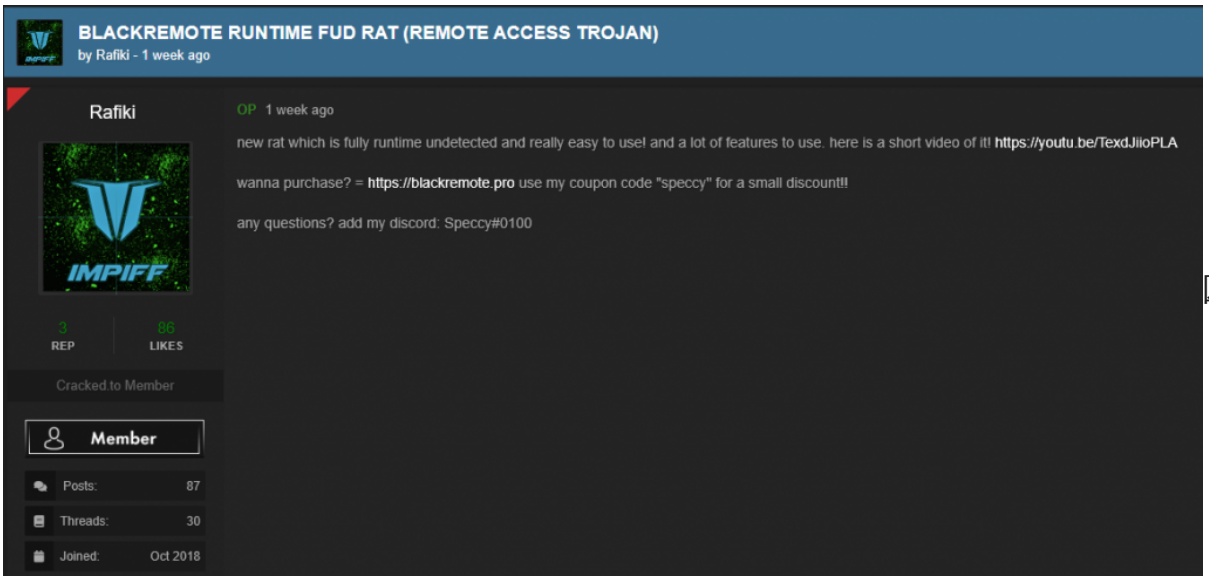


図1 フォーラムで宣伝されたRAT

同じ週、同氏はYouTubeにビデオを投稿（図2）、同ビデオでRATのセットアップ手順を解説しました。

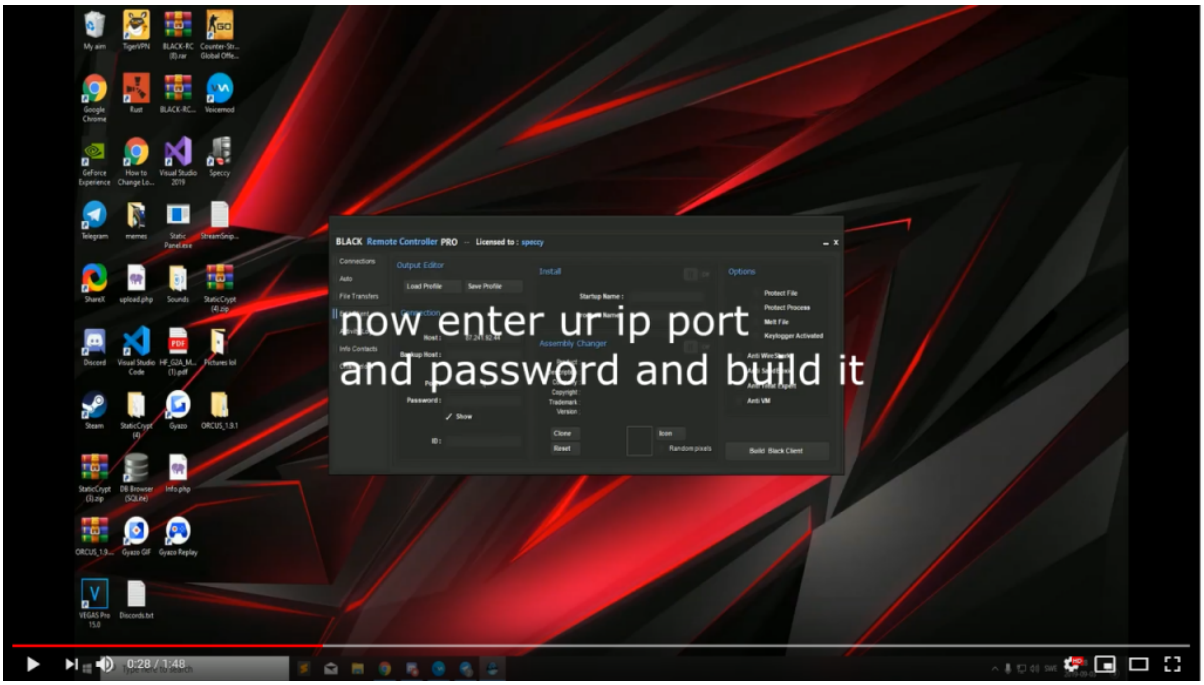


図2 YouTubeの手順解説ビデオ

YouTubeの説明（図3）には、個人サイトspeccy[.]devへのリンクが含まれていました。またこのビデオで同氏は「*このRATは実行時に検出されることがない*」と謳い、「*FUD Cryptorの購入*」リンクを含めていました。ソフトウェアが「検出不能」であることや「暗号化」されていることにはなんら正当な必然性がありません。むしろこうした努力は、マルウェア対策ソフトウェアによる検出防止に向けたものと考えられます。

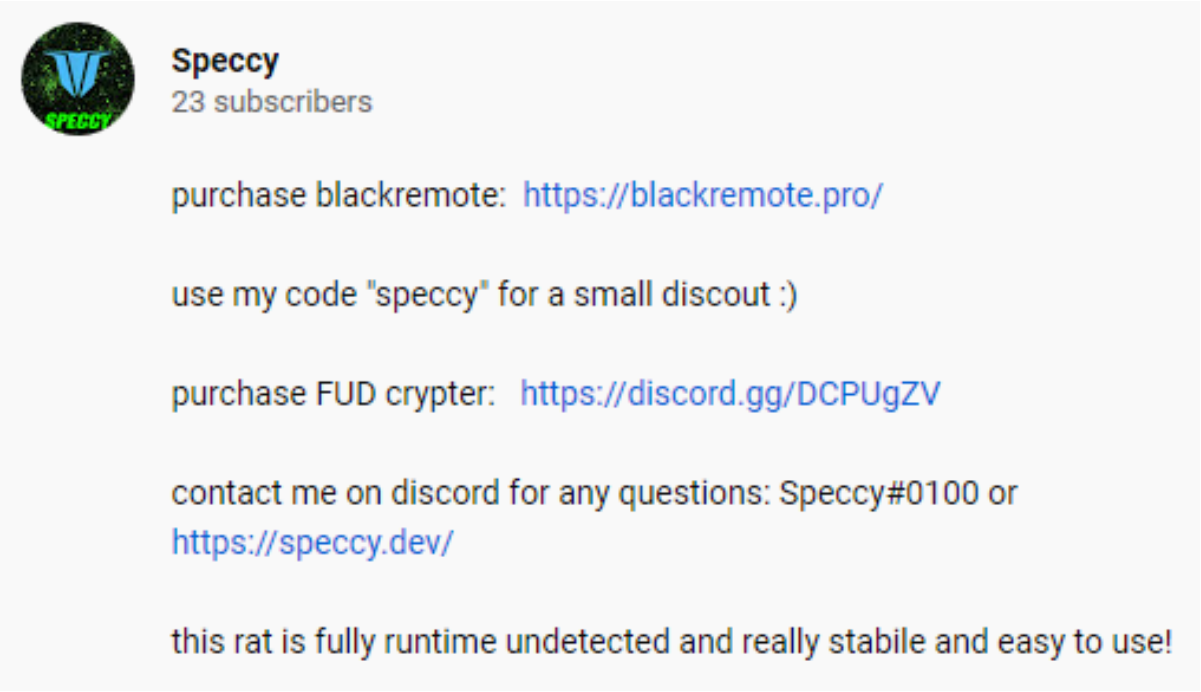


図3

YouTubeの説明

blackremote[.]pro

Blackremote RATの販売サイト blackremote[.]pro（図4）は、2019年8月19日に登録されたものでした。

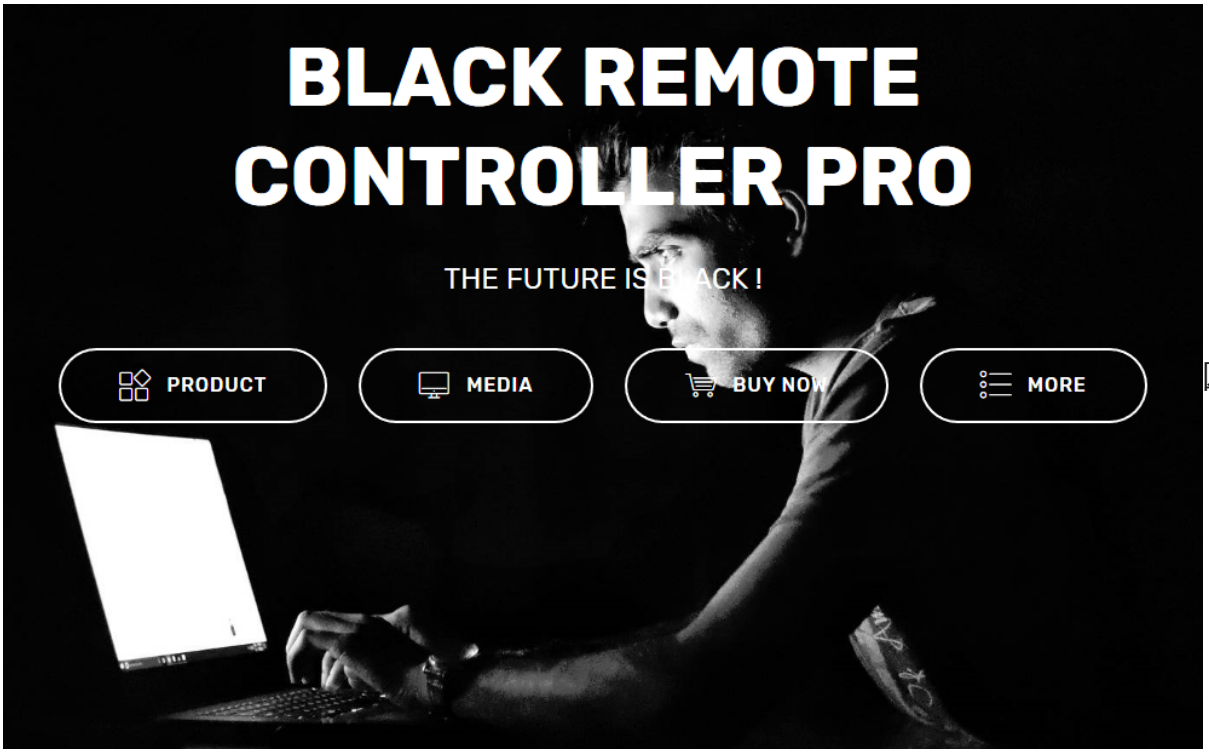


図4

blackremote[.]proSpeccy は、自身のRATについて以下のように説明しています。

「*Black Remote Controller PROはパワフルで多機能なリモートシステム管理スイートです。多彩な機能を誇る本ツールを使うことで、リモートマシンへのフルアクセス、完全制御が可能になります。まるで目の前にマシンがあるかのように、すべての活動・データをリモートから監視、アクセス、操作できるようになります*」

また、同じ地下フォーラムで宣伝されているあまたの攻撃用RATの例に洩れず、Speccyもこのツールの目的が正当なものであることを主張しています。

「*本ツールは、専任の管理者、ペアレンタルコントロール、法医学、監視、リモートアシスタンスなど、さまざまな理由で特定のシステムにリモートからアクセス・監視・操作する必要がある皆さんにとって理想のツールです。Black Remote Controller PRO は、すべてをリモートで行うためのすばらしいソリューションです。*」

ただし、前述の「検出不能」という主張や「暗号化」への言及は、後述する「パスワード回復」機能や「お楽しみ」機能（図5参照）に記載された謳い文句とあいまって、同ツールが到底合法的目的のために設計されたものではないことを示唆しています。

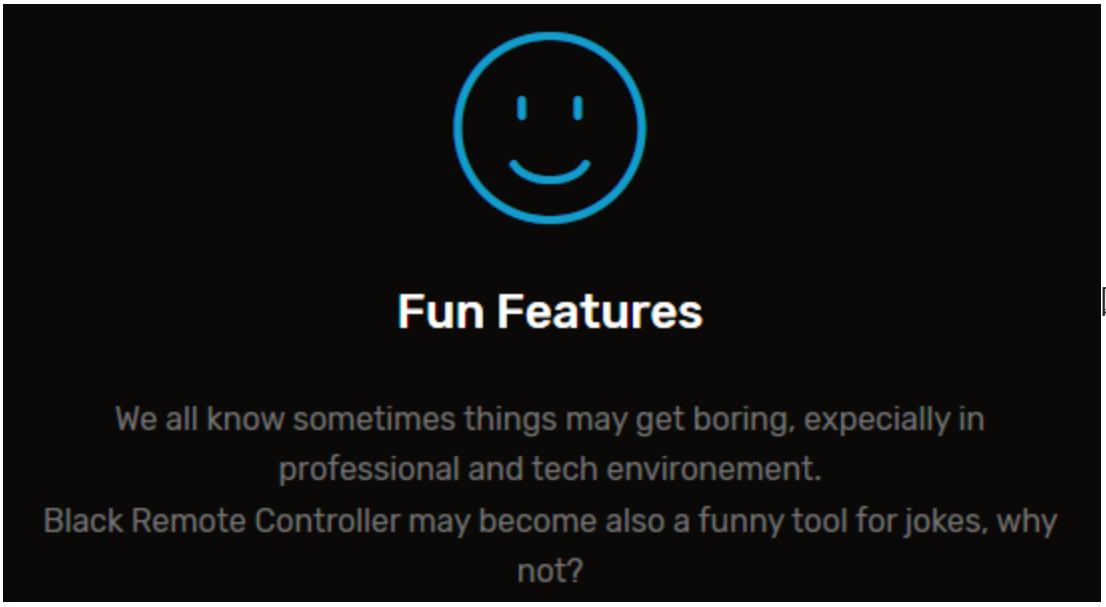


図5 「お楽しみ」機能の説明。(「仕事中やマシンに囲まれた環境でちょっと退屈することってありますよね? そんなとき、Black Remote Controllerは愉快なジョークのタネを提供してくれるかもしれません。そうでしょ?」という説明)

SpeccyのRATライセンスは、他の商用RATと比べて比較的高額で、31日ライセンスが49ドル、93日ライセンスが117ドル、1年ライセンスが438ドルとなっています（図6）。

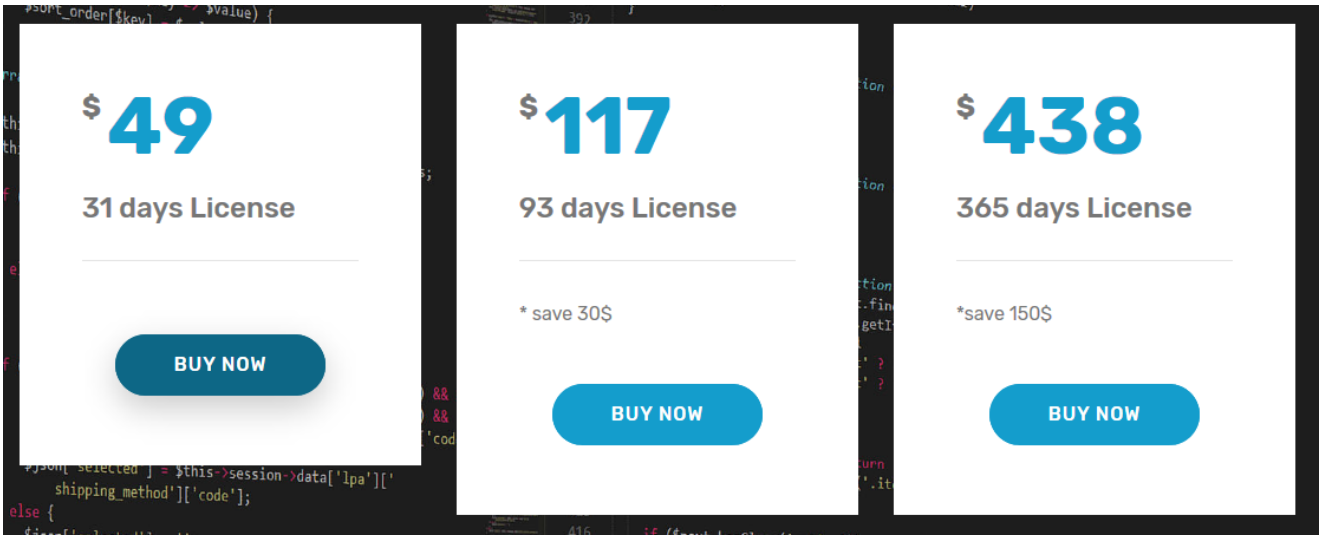


図6 購入オプション
購入はサードパーティの支払いサービスvsell[.]io でさまざまな暗号通貨を通じて行われます（図7）。

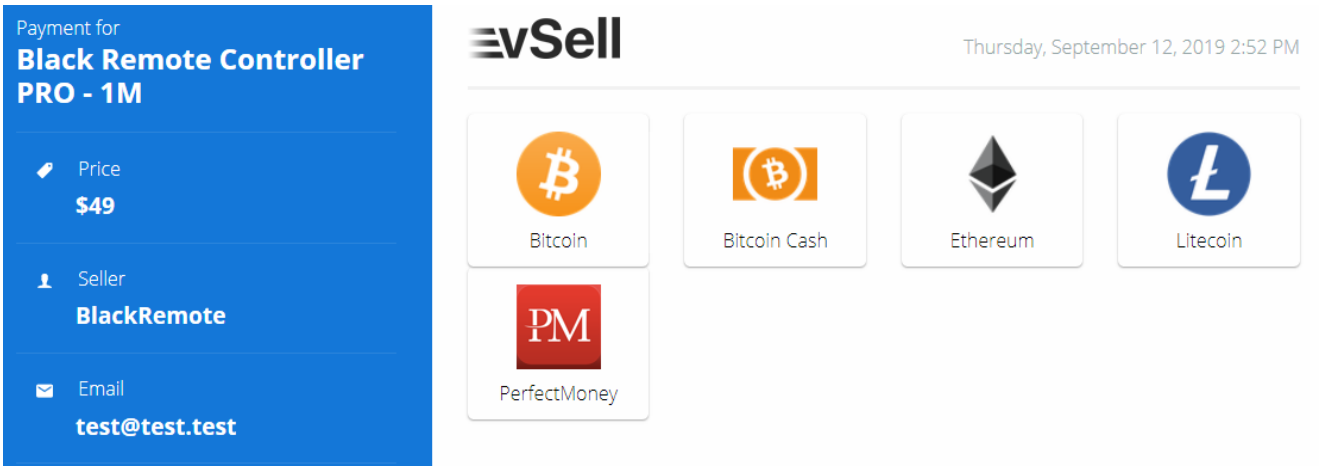


図7 vSell

RATの機能

同人のサイトにはRATの機能が詳細にまとめられています。

リモートデスクトップ
驚くほど低遅延でリモートデスクトップのライブ視聴、スクリーンショット撮影、.aviファイルへのビデオ録画開始が可能。マウスなどのデバイスも制御できます。マルチ画面対応

リモートファイルマネージャー
リモートマシンのすべてのドライブ、ファイル、フォルダをリアルタイムで自由に操作可能。あらゆる種類のファイル操作を実現

リモートウェブカメラ
私物・私有地の監視、ペアレンタルコントロールなど多くのニーズに対応可能。スクリーンショットの撮影や.aviファイルへのビデオ録画開始ができる

ファイル転送
リモートマシンとの間でデータをアップロードまたはダウンロード。同時に複数ファイルの転送をサポート。非常に高速かつサイズ制限なし

キーストロークキャプチャ
キーストロークをライブまたはオフラインモードでキャプチャし後でログを取得。すべてのキーボードをサポート。キーワード検索機能あり

サービスマネージャー
停止中・実行中の全サービスを一覧表示してワンクリックで起動・停止可能

プロセスマネージャー
リモートマシンで実行中のすべてのプロセスの監視、停止、サスペンド、再開。また検出された場合に特定プロセスにアラームを設定することが可能

リモートオーディオ
監視に最適。リモートマシンのマイクデバイスからの音を聞いたり、リモートユーザーの声を聞くことができる

レジストリエディタ
リモートマシンの全Windowsレジストリをナビゲートし、その中のキーや値を取得・変更・新規作成

チャットシステム
リモートマシンユーザーとのチャットセッションを開始、アシスタンスなど必要に応じた利用が可能

システムのシャットダウン、再起動、ログオフ
必要に応じ、リモートマシンをリモートでログオフ、再起動、またはシャットダウン

システムメッセージ
自由にカスタマイズ可能なシステムメッセージ、アラート、情報を作成し、リモートマシンにポップアップ表示

ダウンローダー
自由に保存パスや実行などをカスタマイズし、指定URLからファイルをダウンロードして実行

パスワード回復
リモートマシン、ブラウザ、メールクライアントに保存されているすべてのパスワードを取得。このほかのサポート対象アプリケーションあり

TCP接続モニター
リモートマシンが内外に張っているすべてのアクティブなTCP接続を監視。ポートやプロセス単位、または直接指定してのブロックが可能

webサイトのオープン
サポートなどの必要性に応じ、任意のWebサイトページを起動可能

クリップボードマネージャー
リモートマシンのクリップボードコンテンツに対するアクセス、読み取り、書き込み、または編集を提供

スクリプトツール
スクリプトをリモートで作成・実行。VBS、HTML、バッチ、PowerShellをサポート

スタートアップマネージャ
リモートマシンの全システムスタートアップ項目を管理。複数のスタートアップ方法で項目の追加・削除・変更が行える

リモートシェル
リモートマシンのシェルにアクセスが可能。高度なタスクの達成にはほぼ不可欠な機能

Windowsマネージャー
リモートマシン上で開いているウィンドウ、表示または非表示のウィンドウを管理可能ウィンドウのクローズ、最大化、最小化、非表示、表示、ブロックなど、どんなやりとりでもサポート

インストール済みソフトウェア
どのようなソフトウェアがシステムにインストールされているかを確認でき、リモート環境がどのように設定されているかを確認するさい役立つ

Hostsファイル
Windowsシステムでとても重要な役割を果たすHostsファイルを使い、リダイレクト、ブロック、変換、IP /ホストアドレスの関連付けが可能。たとえばHostsファイルのカスタマイズは一部Webサイトへのアクセス遮断などに不可欠

クライアントマネージャー
インストール済みのクライアントファイルを変更・更新・再起動・強制終了など、多くのオプションあり。クライアントエディタでファイルをカスタマイズ可能」

マネージャー/ビルダー

購入者には、Blackremoteマネージャー/ビルダーソフトウェアのSendspaceダウンロードリンクと6MBのRARファイル用のパスワードが提供されます。マネージャー/ビルダーを展開すると、9MBのメイン実行可能ファイルBLACK-RC.EXE、リソースライブラリ一式、.wavファイル一式を含むリソースディレクトリがインストールされます。

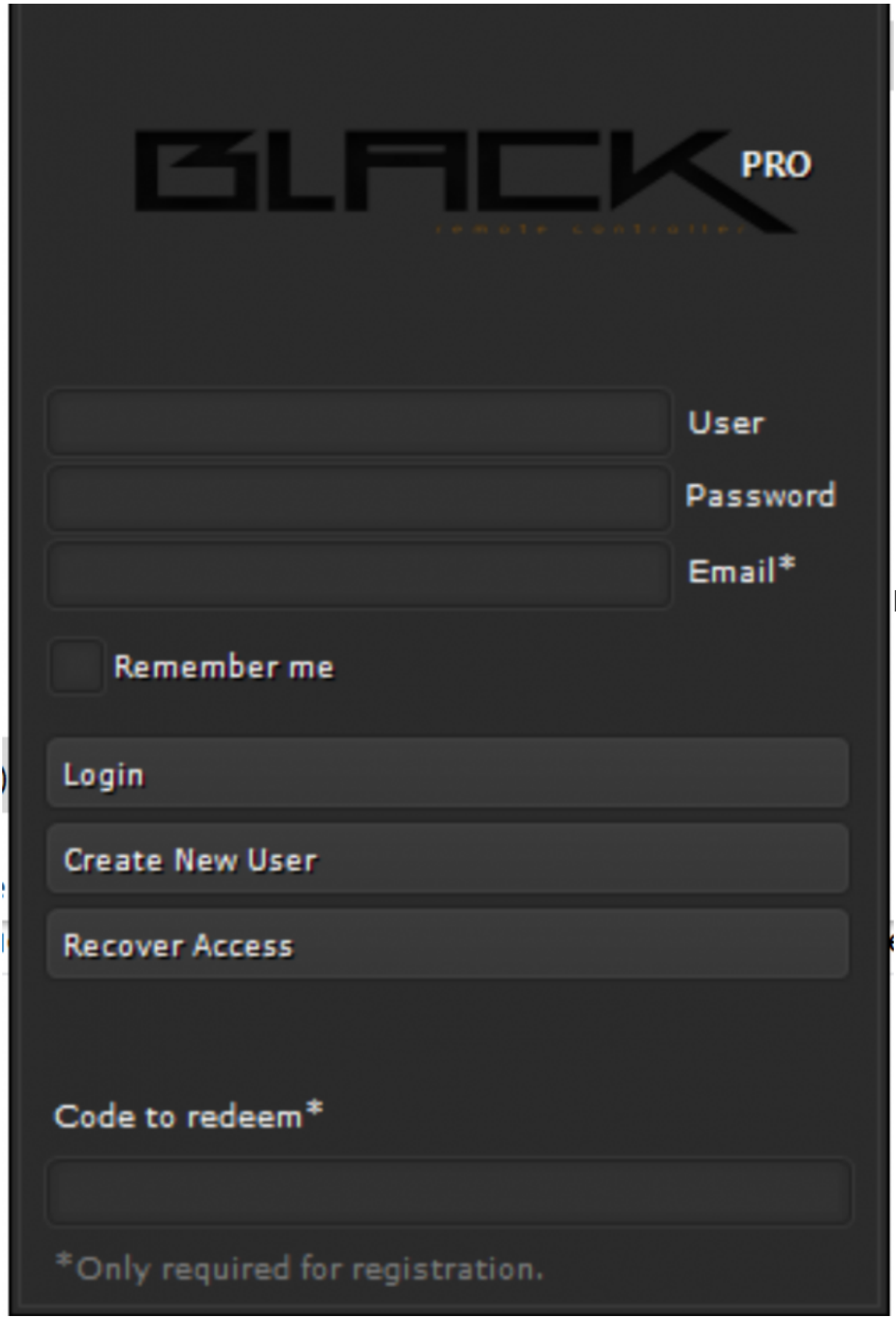


図8 マネージャー/ビルダーの登録/ログイン

マネージャー/ビルダーをロードすると、ユーザーに登録/ログイン画面が表示されます（図8）。Blackremoteはサードパーティの"CodeVEST"ライセンスシステムを利用しており、このライセンスも地下フォーラムで販売されています。ライセンスシステムは、codevest[.]shに接続し、ライセンス有効性の検証を行います。"CodeVEST"は、2017年に停止した"Netseal"に取って代わった商用マルウェア用登録サービスのようですが、"Netseal"の作者Taylor Huddlestonは、自身の商用マルウェア"Nanocore RAT"の販売と"NetSeal"の運用により、2017年に有罪判決を受けました。このHuddlestonという人物は、ほかにも"Codevest"というライセンスサービスを提供したり、"Cyber Seal"という暗号化サービスを提供して利益を得ていました。ここから、商用マルウェアのエコシステム界隈でサービスプロバイダが果たす役割が浮かびあがってきます。つまり、商用マルウェアのエコシステムでは、マルウェア販売者だけでなく、マルウェア販売に付随するライセンスサービスやマルウェア販売者が検出回避目的で購入する暗号化サービスなども、商用マルウェアエコシステムで一翼を担っているということです。

図9
CodeVEST

Blackremoteマネージャー/ビルダー（図10）を使用すると、ユーザーは自身が構成したとおりに新しいクライアントマルウェアを構築し、感染クライアントからの接続を制御することができます。

図10
Blackremoteマネージャー/ビルダー

ユーザーはマネージャー/ビルダーを使用してクライアント接続（図11）、接続ログ（図12）、接続クライアント一覧表示（図13）など接続時のアクションを定義することができます。

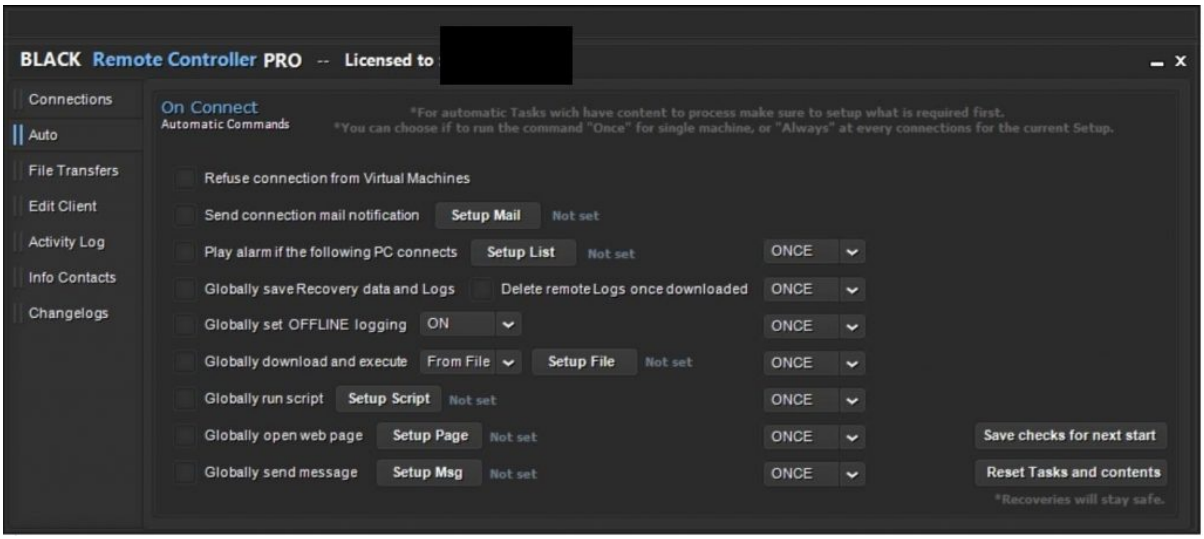


図 11 接続時のオプション

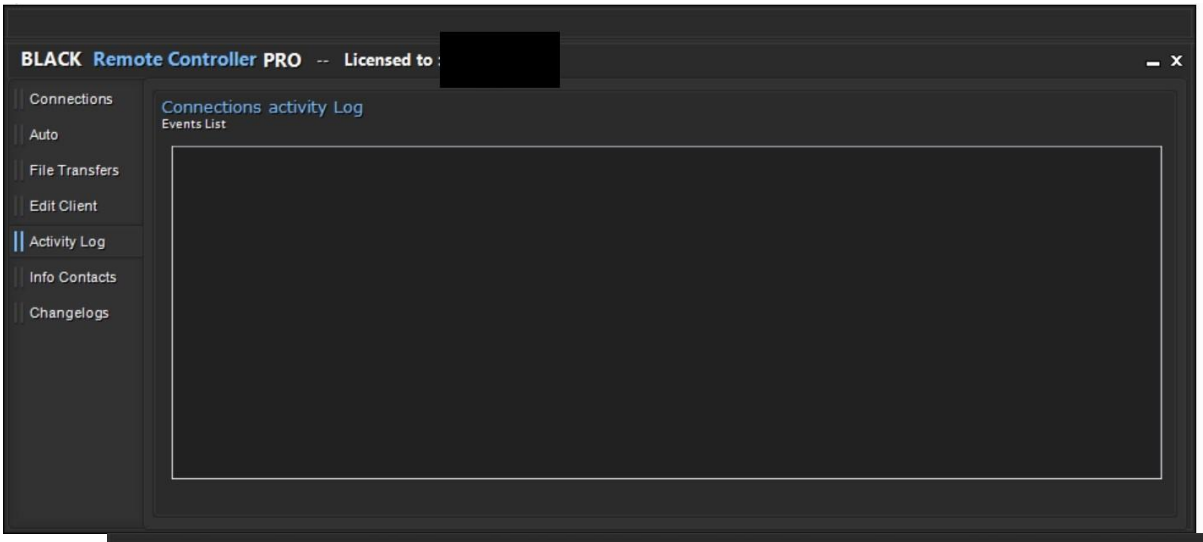


図12 接続ログ

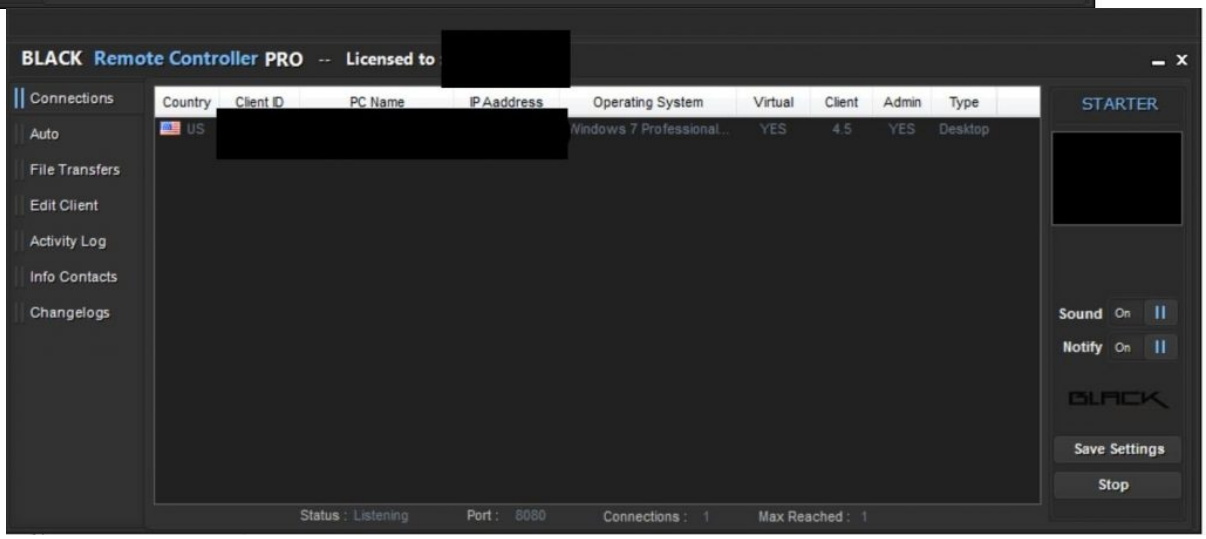


図 13 アクティブな接続

Speccyが宣伝しているクライアント制御機能は、接続クライアント用のコンテキストメニューに表示されます（図14）。

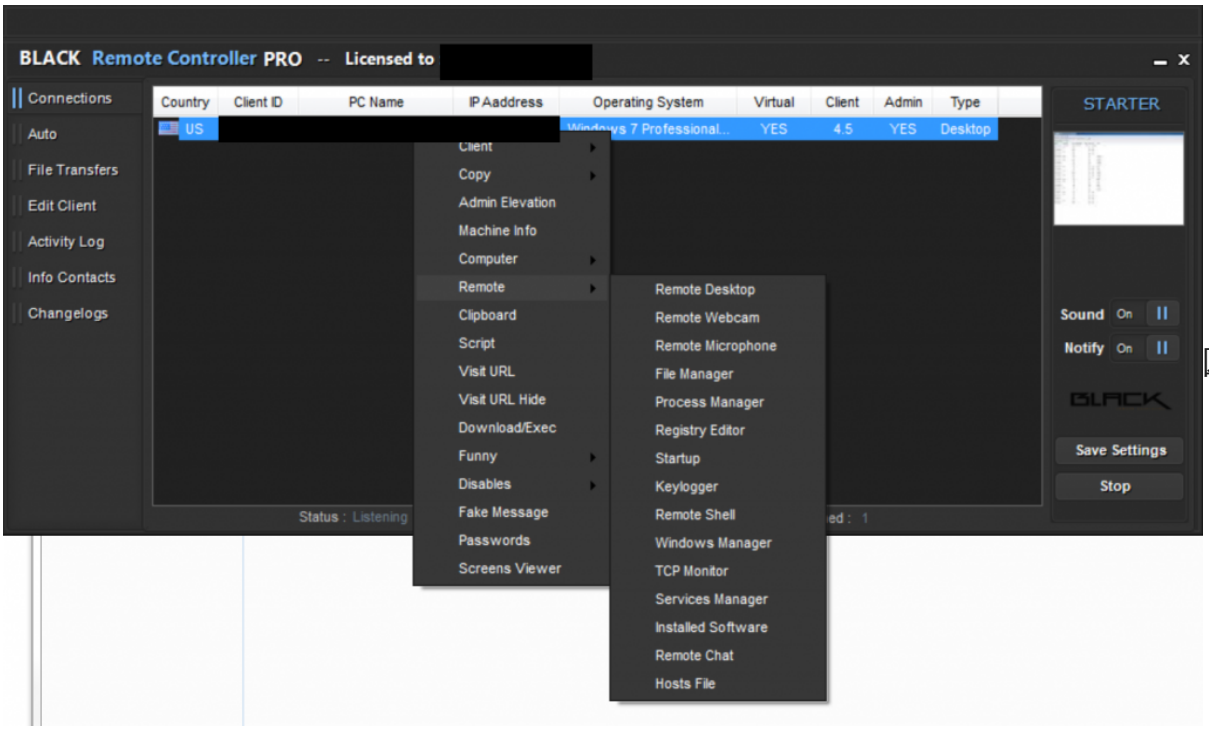


図14 クライアント制御

Speccyは同ソフトウェアの開発を活発に続けています。changelogsを見ると、新規にクライアントの権限昇格機能が追加されるなど、定期的に少しずつ機能が拡張されている様子がうかがえます（図15）。

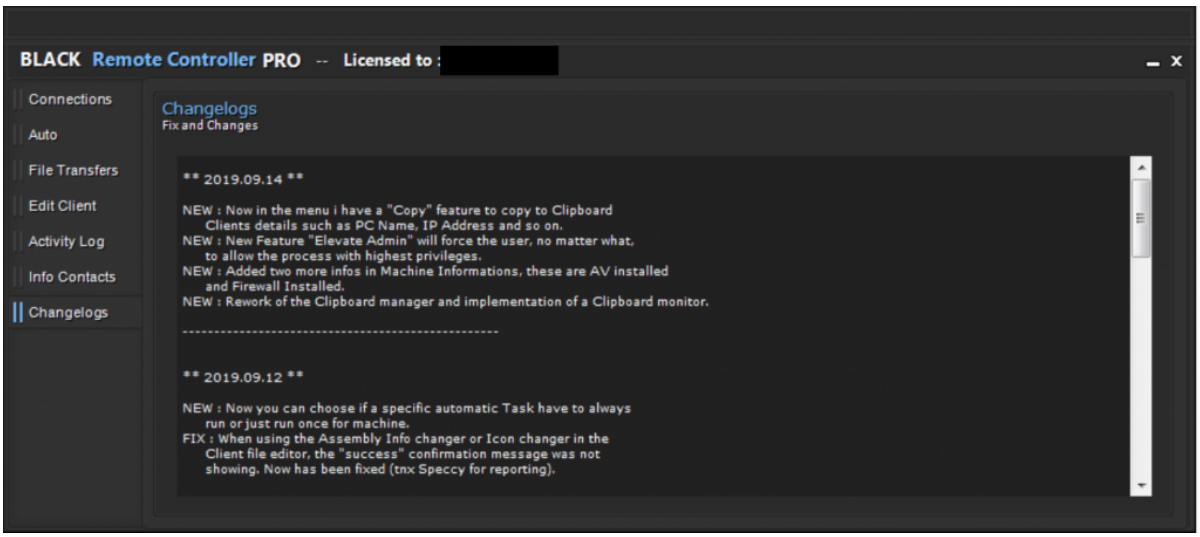


図15 Changelogs

クライアント

私たちは、同じような時期、同一のファイルサイズをもつ複数の異なるサンプルが観測されたことに気づきました。このことから、「C2情報やRATオプションの種類などの動的コンテンツとは無関係に、クライアント作成時の難読化プロセスにより、ある特定のバージョン単位で、Blackremoteのクライアントはすべてファイルサイズが同一になるのではないか」

と私たちは考えています。ビルダーもクライアントも、複数の難読化ツール（Agile.NET、Babel.NET、Crypto Obfuscator、Dotfuscator、Goliath.NET、SmartAssembly、Spices.Net、Xenocode）を使用して厳重に保護されています。

利用の実態

Blackremoteはごく最近のマルウェアですが、本稿執筆時点ですでに実際の攻撃に使用されていることが確認できています。Speccyが自身のBlackremote RAT販売を開始して1ヶ月で、2200件以上の攻撃セッションが弊社顧客ベースに対して行われ、50個ちかくのサンプルが観測されています。

Blackremoteの顧客

興味深いのは、これらの攻撃の大部分がある1つの攻撃キャンペーンに帰する点です。doc00190910.exeというファイル（SHA256：2b3cda455f68a9bbbeb1c2881b30f1ee962f1c136af97bdf47d8c9618b980572）がメールで拡散されており、そのピークは2019年9月9日から11日にかけてでした。同メールは世界中のさまざまな業種（図16）のパロアルトネットワークス顧客をターゲットにしていました。コマンド&コントロールサーバー（C2）にはrenaj.duckdns[.]org (103.200.6[.]79) が使われています。同C2は1800件を超える攻撃セッションで使用されていました。

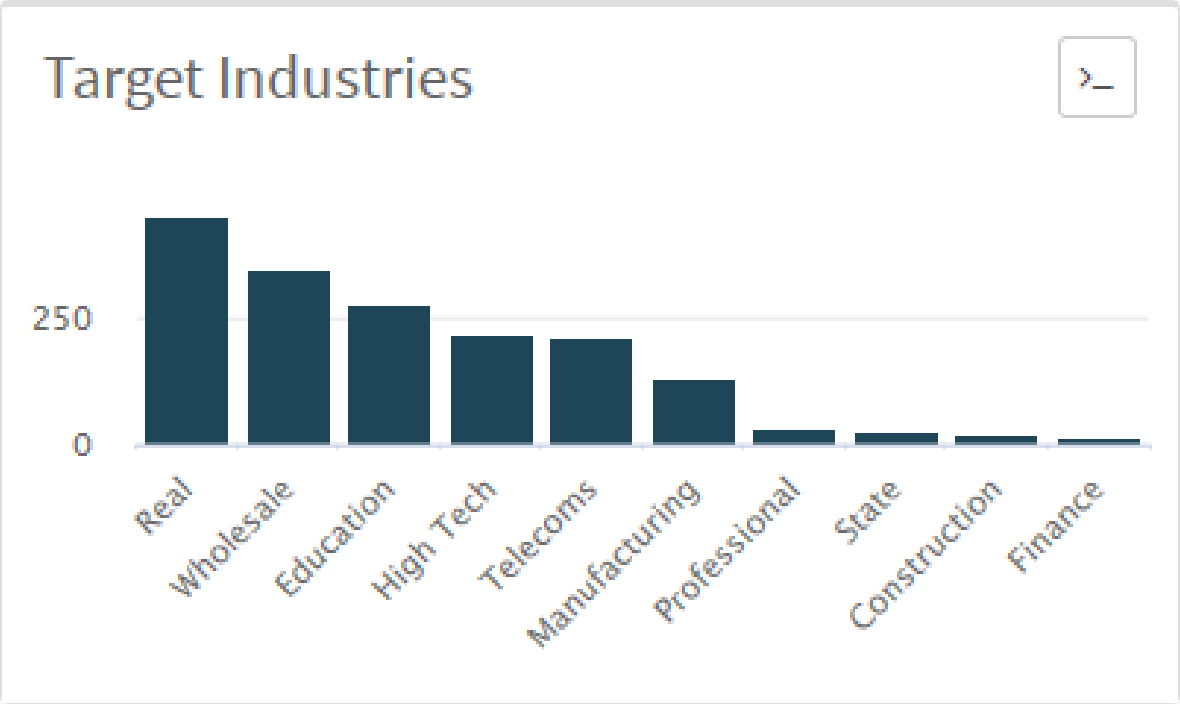


図16 攻撃キャンペーンの対象業種

同じC2は、2018年初頭まで遡って50件以上にわたるNetwire、Nanocore、Quasar、Remcos商用RATサンプルによって使用されていたことが確認されています。このことからは、悪意のあるサイバー攻撃用の手段を提供しつつ、Blackremoteを含む商用RAT作成者たちがどのようにして利益を得ているのかがわかります。

結論

商用RATの多くは、インターネット上で長年にわたって販売されます。こうした商用RATの作者たちは、悪意のある攻撃者たちにRATビルダーで作成した何千ものマルウェアサンプルを拡散する手段を提供することにより、利益を上げています。出現したばかりのRATを数日以内に文書化し、その背後にいる人物（この場合はスウェーデン出身の18歳）を特定する機会があれば、しかるべき法執行機関が、同人物とその顧客に対し、タイムリーに行動を起こすことができるでしょう。Unit 42は、Blackremoteの開発者個人を特定しています。ここで同人の身元に関する情報を共有することは避けますが、しかるべき規制当局には情報提供を手配済みです。

商用RATが長期間販売されれば、同RATを使ったサンプルがそれだけたくさん作成されるだけでなく、ほかの攻撃者が同RATを解読して無差別に配布する機会もまた増えてしまいます。できるだけ早い段階でこうしたマルウェアの販売を特定・阻止することで、マルウェアの拡散を防ぐことが重要で、それは技術力の低い別のアクターたちの攻撃の芽を摘むことにつながります。

優れたスパムフィルタリング、適切なシステム管理、最新のWindowsホストを導入している組織については、同脅威への感染リスクはかなり低いでしょう。

パロアルトネットワークス製品をご利用中のお客様は同脅威から保護されています。

- 弊社のThreat Preventionプラットフォームでは、WildFireとTrapsでBlackremoteマルウェア ファミリを検出します。
- AutoFocusをお使いのお客様は次のタグを使用してこれらの活動を追跡できます: Blackremote

パロアルトネットワークスは本稿で見つかったファイルサンプルや侵害の兆候などをふくむ調査結果をCyber Threat Alliance(CTA サイバー脅威アライアンス)のメンバーと共有しました。CTA のメンバーはこのインテリジェンスを使用して、お客様に保護を迅速に提供し、悪意のあるサイバー攻撃者を体系的に阻害することができます。Cyber Threat Allianceの詳細については、www.cyberthreatalliance.org のWebサイトをご覧ください。

ハッシュ値

514b3d98c1a8cbd5ea08ff31e22700adb9ca0d93d9bc4d6a5232324f0f3e806d
39721fb2d55777eeb6bdfdc9068782894993d172bb92cbad6a525c130312ef11
c3075bced2e864ee7e693c19ecf1ed82cde0aae3d440e9ff2f37d3d6e20fdf0f
3eda427ad5816e6dcf077562a367f71e8bdf5aa931e594416ae445357c12b409
3265bb60b532005bc3535bdf7336bff1845aa5ed3306fd5dbb2ec884cb3d6323
744438c125ceb7a3a7e44cca9fd6b397e982d048f680f164abd46743fd64cd12
33a34ae9a757f6be754571e752a3ee9200153db16c34cf2fd5590ad616fbb04e
fb8b9fe377ccdef76645a081905137e3580eed1defdabbbf48a3d20f0dc760b4
0278145549af5cad9318d51e4c150afe2180b55f72194562885d5c8f9526f465

ea5384db27a27b826c100bbc2535561ea61bf4f44eb4eb93243740188799d675
123539b0eaff1a23606d3716cdc0c73618af6f0cd821ae33863d0f47b2267dbf
f7b165903f6f9b979e84399ce4e1b85ed2927740771d85a7b8c85203641a08a1
93bfbd4b12a17732c8b7e66c554f98187184c6d845bd02e0dbb2104ce8da0453
469d8b2cced859f57b535363307c1e29c0bf0342d14ce0da109a40493a441b62
ada653c948875a9c1ca588251b317d8e971fdf980252d92e36d59f14f5eb9ab9
c207cf50305f126451e2dc5493d83614fdf801541d011e5002ee5daea2b4433b
57a15cc236e4d2ba6e08b062a75671b8a674e0d8498d87e48652c778ea263d49
3875545099276f2b34c3752b177b6d90a2eeb47148ddfb559a4d076d0f40716a
e1bf5d2ef3a4f922f9a15ab76de509213f086f5557c9e648126a06d397117d80
ed7693d9b1b069d39451002bc1df06bf4e123926fa34abb6afeb9a18d6d90dcd
901e06cd91adb7255d75781ef98fac71d17f7bed074a52147bdbd42ea551b34f
9c93b768b5261194ad207c0e92e9767e70ba38203f24f2909e1b39a9a1d6570c
129491bfdd9a80d5c6ee1ce20e54c9fb6deb2c1e1713e4545b24aa635f57a8b9
931839ee649da42b0ee3ac5f5dfa944b506336c7f4e5beb3fc07a6b35a7e6383
0908f8fbe1e3a77d941ae83fe3677d103d86d6e59a6ae4530eadba8af7fc1b3a
69aaaf148a132385512f66d7668b045d6467f8639a3ef7460e20ce0627bc84fc
f6ae66a8a6357d7622463db9953ae164d496e7f5ee0dfe2c8e3550a231f25078
c5a78bf01ab2e44c7dba3a363f2eda51cf648e904f2beb47d6cf3112368ff20c
f83e25cf2b2c2f2d0a14e3f538c11f70135ee8ec158446a51bb0f2d999765267
cb423b73ae3e51195abbcf8bc1f2655d61436825815089b92e843b570ac7c86d
ee20db296c7c4cf3ca6db0c739f1579f554a447b6c1e2b343b22d341f288662f
a4bc7d42dd64df3502b7f8c2335c64eba7a484479fc8c2dc8a4aa448f10354b3
756efcbd2767c5499b6f09a089033c82050459fc2999d3ce79caa25746693e26
117cf46ae69134dbe0c8a1d5f4cac92b46c15ea4945929df3880c0ac63e158f3
e5366365852a953a1747ab8a5d721c2536c5671c07bfecf648fb2cf6a13f2dc0
0c63983cb38d187c187f373852d7b87ff4e41ea0d77d75907aa3388ad957f38f
e54531896dbd100fec41cfc89b06f2afa1efd4077d1f197b1b88f74371135436
c38006115bd7c22151c4e31d8d4ed6ec114c2aaf1c7c0da12ef7b44f96fc58d6
0f66acc9883b284580980020d4a48557b2fe38312ca80db97c77cc2fa78c51fb
77fe670ed011e547db72207ba5849b9f618185b52e0ae766c23ef675b116b252
2b3cda455f68a9bbbeb1c2881b30f1ee962f1c136af97bdf47d8c9618b980572
105cab9c9604238c05be167c6d8d47cd2bc0427b07ede08c5571b581ebd80001
cc795b94cac222afc69749359d8b17d9fb7a7fb6e824d43008c1674c0d146929
1737cf3aec9f56bb79a0c4e3010f53536c36a1fbeeedea81b6d7b66074ecffbe