Secureworks®

脅威インテリジェンス エグゼクティブレポート

Volume 2022, Number 2

カウンター・スレット・ユニット™（CTU）
リサーチチーム

エグゼクティブサマリー

セキュアワークスのカウンター・スレット・ユニット（CTU™）リサーチチームは、セキュリティの脅威を分析し、企業や組織のシステム保護を支援しています。2022年1月から2月にかけて観測された脅威のふるまい、グローバル規模の脅威状況、セキュリティトレンドをもとに、注目すべきポイントをCTU™のリサーチャーがまとめました。

- **侵攻開始直後の1週間、ロシアによるサイバー攻撃ではウクライナが集中的に狙われた**
- **GOLD ULRICKおよびContiの内部情報が流出**
- **ダウンロードされた法的文書に埋め込まれていたローダー**

侵攻開始直後の1週間、ロシアによるサイバー攻撃ではウクライナが集中的に狙われた

ウクライナ侵攻直前から侵攻開始後の第1週にかけてロシアのサイバー部隊が行った活動は、標的をウクライナ国内に限定したものでした。ウクライナ以外の国や地域の大半の組織にとっては依然としてランサムウェアが重大な脅威であることに変わりはないものの、この間、ロシア政府を後ろ盾とするサイバー活動による影響はほぼ皆無でした。ロシアによるサイバー活動の激化に備え、ランサムウェア攻撃の緩和を目的としたセキュリティコントロールを実装することが最善の予防対策です。

ロシアがウクライナ侵攻に先立ち軍備増強を開始した1月以降、「2017年に世界規模の被害をもたらしたNotPetya攻撃のように、ロシア側が自己拡散型のデータ消去マルウェアを使った攻撃を仕掛けてくるのではないか」という懸念が広がりました。しかし侵攻の初期段階で発生したサイバー攻撃はウクライナ国内の組織を狙ったものと見られたため、こうした懸念は杞憂に終わりました。ロシア軍によるウクライナ侵攻の直前（2月23日～24日）、ウクライナの行政・金融機関に対する分散型サービス拒否(DDoS)攻撃やデータ消去マルウェア攻撃が発生しました。今回のデータ消去マルウェアは、あっという間に広がったNotPetya攻撃とは異なり、標的ネットワークへの接続状態を長時間維持した後に展開されました。ウクライナに対する今回と同様の攻撃（DDoS攻撃やウェブサイトの改ざん）は1月中旬および2月上旬にも発生していますが、ウクライナ以外の国や地域の組織にとっては引き続き、通常の金銭目的のランサムウェア攻撃のほうが重大な脅威であることに変わりません。

ロシアは過去にも、サイバー部隊の力を物理的な攻撃の補完手段として使用し、敵対視する国々にダメージを与えてきました。2008年には、グルジア（現ジョージア）の一部である南オセチア地区への侵攻直前に、ロシアのサイバー部隊が同国に対してDDoS攻撃、ウェブサイト改ざん、大規模なスパム攻撃を実行しました。また、2007年と2009年にはロシア国内の攻撃グループによるエストニアおよびキルギスタン（現キルギス）へのDDoS攻撃もそれぞれ確認されています。こうした攻撃は、標的国にパニックを引き起こし、標的国政府の信頼を失墜させ、基幹インフラの

運用を妨害し、民衆の決意を揺るがすことが目的です。ウクライナへのサイバー攻撃も今回が初めてではありません。2015年12月と2016年12月にロシアの攻撃グループIRON VIKINGがウクライナの電力網に対して仕掛けた破壊的攻撃などはよく知られています。

西側諸国の制裁によってロシアが孤立を深めるにつれ、ロシアのサイバー部隊が無差別にその力を行使する可能性が高まるかもしれません。また、ロシアの基幹インフラを破壊する親ウクライナ派の攻撃グループへの応戦として、ロシア国内の犯罪集団や活動家集団などの攻撃グループが報復攻撃を重ねる恐れもあります。刻々と変わるウクライナ情勢では次に何が起こるかわからないため、ランサムウェア攻撃およびDDoS攻撃の緩和を目的としたセキュリティコントロール対策を重点的に講じることが、最善の備えと言えるでしょう。具体的には、パッチの適用、多要素認証、ネットワークのセグメンテーション、DDoS攻撃緩和サービスの契約、エンドポイント検知・対策ソリューションのデータを監視すること、などが挙げられます。

上記を踏まえ、ぜひ実行してほしいアクション：
当社では、刻々と変わるロシア・ウクライナ情勢に関する最新情報をこちらのマイクロサイトに掲載しています。ぜひブックマークしてください。

GOLD ULRICKおよびContiの内部情報が流出

今年2月、ランサムウェアContiに関する内部情報が暴露されたことで、Contiの運営元であるサイバー犯罪グループ「GOLD ULRICK」の運営実態が見えてきました。しかし、これがきっかけでランサムウェア全般の脅威が軽減される可能性は低いため、今後とも警戒を怠らないようにしましょう。

Ransomware-as-a-Service（RaaS）の構成要素であるランサムウェアContiを運営するサイバー犯罪グループGOLD ULRICKは2月25日、「我々はロシアを支持する」と大々的に表明し、ロシアを狙ったサイバー攻撃に応戦する構えを見せました。同グループは2月26日に、この声明を「我々が支持するのはロシア政府ではなく、ロシア国民である」という内容に修正しましたが、トーンが控えめになったからといって、すべての人々が納得したわけではありませんでした。

2月27日以降、@ContiLeaksと名乗る新なツイッターアカウントが、同グループの内部情報を次々に暴露しています。暴露されたデータには、グループ内部でのチャット履歴、組織構造、ランサムウェアのソースコードや攻撃の詳細、被害組織との交渉記録などが含まれています。当社CTUによる分析の結果、このデータを流出させた人物はGOLD ULRICKの戦争に対する姿勢に不満をもつ内部構成員やその傘下にある加盟メンバーの構成員ではなく、ウクライナ人のサイバーセキュリティ研究者であることが示唆されています。情報流出の目的は、内部で猜疑心をあおり、内部分裂を生じさせることであると考えられます。また、これを機に一部の加盟メンバーが別のRaaS運営組織に鞍替えする可能性もあります。

2019年11月に登場したContiは、最も活発なランサムウェアファミリーのひとつです。2月末現在、Contiの暴露サイトには729社の被害組織名が掲載されていますが、身代金を支払ったため表面化していない被害組織も数多く存在すると見られます。支払われた身代金の平均額は65万ドルを超えるという報道もあります。2021年後半以降、GOLD ULRICKは攻撃の戦術・手法・手順（TTPs）を一部変更し、初期アクセスの攻撃手法（IAV）として使っていたTrickBot（現在は休眠状態となっているマルウェア）の代わりにEmotetを使用して悪質なペイロードを配信するようになりました。また、GOLD CRESTWOODにEmotetを使った活動を再開するよう促したのはGOLD ULRICKであるという報道もあります。今回流出した内部情報を見ると、GOLD ULRICKが他のサイバー犯罪グループとどれほど密接な関係にあるのかがわかります。また、採用形態や人事査定、報酬条件などがごく一般的な企業と同様に体系化されており、相当な規模で組織化された犯罪グループであることも見てとれます。

GOLD ULRICKの内情が暴露されたのは今回が初めてではありません。2021年8月には、Conti攻撃に用いる様々なツールが一覧化されたプレイブックが流出しましたが、消滅することなく活動を続けています。また、2021年5月にアイルランドの公的医療サービスに対して実行された同グループの攻撃を受け、アイルランド国家警察、ユーロポール、インターポールによる合同摘発作戦が同年9月に展開されましたが、その後も活動を続けています。

ロシアとのつながりをもち、ロシア支持を公言しているランサムウェア攻撃グループはGOLD ULRICKだけではありません。しかし、LockBitの運営元であるGOLD MYSTICなどは「政治には関心がない」として、「我々は、様々な政治的見解をもつ個人が集まった多国籍チームで活動している」と宣言しています。一般的に、サイバー犯罪グループの多くがロシアとのつながりをもっているとされていますが、その大半は「一に金銭、二に政治」という動機で活動しています。

今回の情報流出がランサムウェアContiの運営に与える影響を具体的に判断するにはもう少し時間が必要です。GOLD ULRICKの暴露サイトには3月上旬現在でも、これまでと変わらず新たな被害組織が掲載されており、ランサムウェアによる全般的な脅威レベルが軽減する可能性は低いでしょう。ロシアによるウクライナへの攻撃がもたらす先行き不透明感と合わせて考えれば、セキュリティ対策や警戒の手を決して緩めてはならないことは明らかです。

上記を踏まえ、ぜひ実行してほしいアクション：
ランサムウェア攻撃やデータ消去マルウェア攻撃に対処できるよう、
社内の事業継続計画および復旧プロセスを再確認しておきましょう。

ダウンロードされた法的文書に埋め込まれていたマルウェア

一見ごく普通のウェブサイトでも、そうではないことがあります。ユーザーが警戒すべきは、添付ファイルやリンクが含まれる迷惑メールだけではありません。たとえ正規のビジネス文書のように見えるコンテンツであっても、ウェブサイトから情報をダウンロードする際はその内容に充分注意を払う必要があります。

今年2月、サイバー犯罪グループGOLD ZODIACが法的文書や財務資料を配信する正規のサイトを装ったウェブサイト経由でマルウェアを展開しようとしていたことが当社CTUリサーチャーの分析によって判明しました。同グループはJavaScriptベースの「Gootloader」の配信を目的として、侵害されたWordPressサイトを複雑にネットワーク化し、自作のブログ記事を掲載していました。Gootloaderに感染すると、複数のマルウェアファミリー（ランサムウェアLockBitなど）が展開される仕組みになっていました。

この攻撃グループは、検索エンジン最適化（SEO）を悪用するSEOポイズニングという攻撃手法を使い、侵害されたサイトの検索順位を上げていました。よく検索に用いられる法令・財務関連のキーワードを埋め込んだコンテンツを侵害されたサイトに掲載して来訪者を安心させ、法的文書や財務資料に見せかけたGootloaderをダウンロードさせるという手口でした。

この手口は、被害者に「迷惑なフィッシングメールが誘導するダウンロード先ではなく、正規のインターネット検索を通じてダウンロード対象ファイルを見つけた」と思い込ませる巧妙な手法です。そのため、ソーシャルエンジニアリングの検知に関する従来の対策トレーニング項目の大半をすり抜けることができます。組織を守るには、従業員に「フィッシング攻撃やマルウェア拡散攻撃はメール以外の経路でも発生し得る」という点を周知徹底することが大切です。また、信頼性のないサイトや、マイナーなサイトからファイルをダウンロードする行為も危険です。信頼性の無いサイトや、マイナーなサイトからファイルをダウンロードする行為も危険です。こうした脅威は、開設してから日が浅いサイトへのアクセスをコントロールする、または外部の脅威インテリジェンスデータを取り込むことで緩和できます。ただし、これらの対策だけでは包括的な保護策とはなりません。

WordPressなどのコンテンツ管理システム（CMS）を利用する組織においては、CMSソフトウェアへの迅速なパッチ適用が不可欠です。また、プラグイン製品の脆弱性も攻撃グループに悪用される恐れがあるため、外部のプラグイン製品へのパッチ適用も忘れずに実施しましょう。

上記を踏まえ、ぜひ実行してほしいアクション：
社内ユーザーのセキュリティ意識を高めるために、新たな脅威を想定した、包括的なトレーニングを実施しましょう。

結論

本書の公表日現在、ロシア・ウクライナ情勢に関連するサイバー活動は標的が明確に絞られていますが、紛争の展開次第で標的が変わる可能性もあります。ウクライナ以外の国や地域の組織にとっては、通常のランサムウェア攻撃やサイバー犯罪グループによる脅威のほうが大きいため、今後とも脅威の動向を注視し、最新状況を把握することが不可欠です。

CTUリサーチチームについて

CTUのリサーチャーは、メディアでも頻繁に取り上げられ、セキュリティコミュニティ向けの技術分析を公開し、セキュリティカンファレンスでは新たな脅威について説明しています。セキュアワークスの高度なセキュリティテクノロジーと、業界でのネットワークを活用して、CTUリサーチチームは脅威アクターを追跡し、異常なアクティビティを分析して、新しい攻撃手法と脅威を追跡しています。このプロセスにより、CTUのリサーチャーは、脅威をすぐに識別し、損害が生じる前にお客様を保護する対策を開発します。

リサーチ

お客様が直面する脅威の根本を理解し、対処・保護するための対策を作成

インテリジェンス

ネットワークエッジを超えて、脅威の可視性を強化する情報を提供

統合

CTUによるリサーチとインテリジェンスを、セキュアワークスのマネージド・セキュリティ・サービスとコンサルティングに投入

Secureworks®

Secureworks®（NASDAQ: SCWX）は、サイバーセキュリティにおける世界的な先進企業です。当社ソリューションをご活用いただくことにより、お客様やパートナーは攻撃者よりも常に先手を打ち、マーケットに迅速に対応し、ビジネスニーズを満たすことができます。クラウドネイティブのSaaSセキュリティプラットフォームとインテリジェンス主導のセキュリティソリューションの独自の組み合わせにより、20年以上の脅威インテリジェンスと分析から得た深く広い知見を提供しております。このように、長年にわたるサイバー攻撃の最前線で蓄積した実践経験に基づく知見を提供するセキュリティプラットフォームは、唯一無二のセキュアワークスだけです。

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
www.secureworks.com

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs Forest,
Sydney NSW Australia 2086

日本
東京都千代田区大手町一丁目2番1号
Otemachi Oneタワー17階
www.secureworks.jp

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom

1 Tanfield
Edinburgh EH3 5DA
United Kingdom

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111

緊急のインシデント対応に関するご相談は、こちらまでご連絡ください。

03-6848-9760

