アンラボ・セキュリティレター

Press Ahn

2022.6　Vol.102

ハッキングの温床 「ダークウェブ＆ディープウェブ」 に一体何が？

ダークウェブ&ディープウェブ動向報告書 (2022 年 1-3 月期)

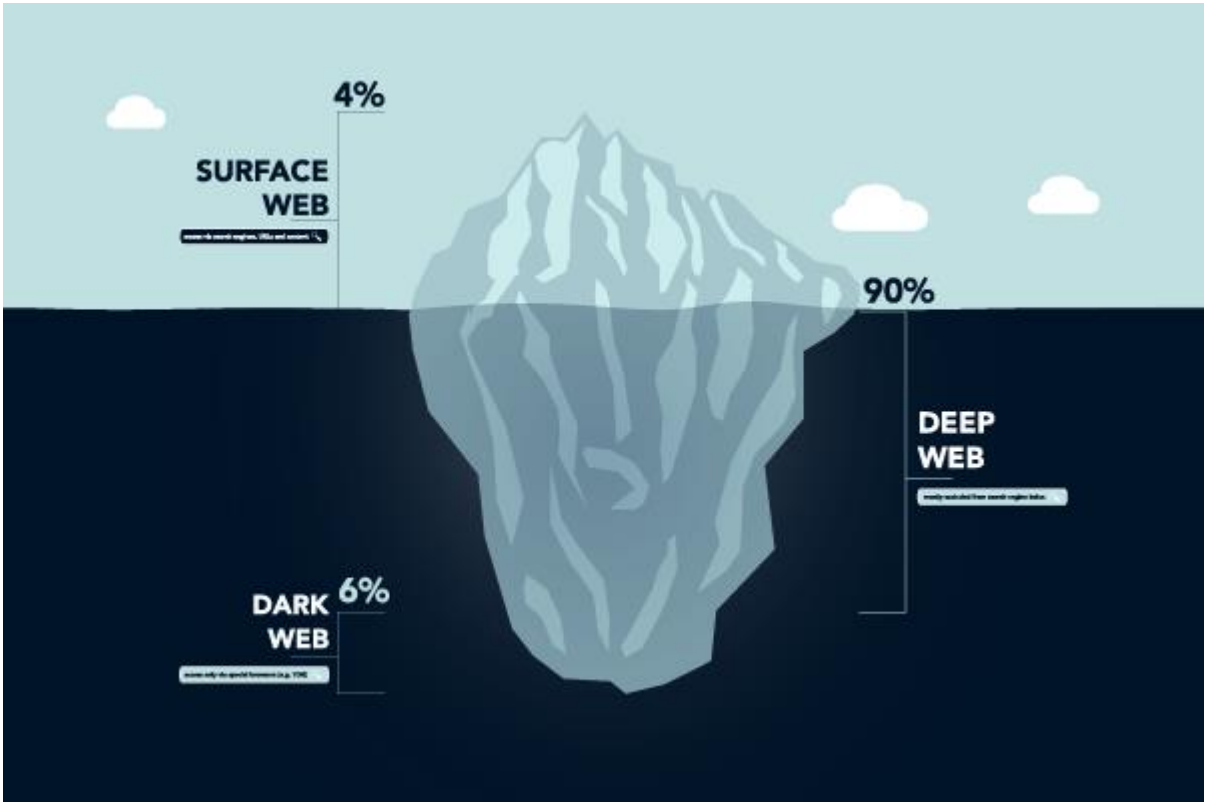
ハッキングの温床 「ダークウェブ&ディープウェブ」 に一体何が？

2022年 1-3月期は、米ロ新冷戦の激化とロシアのウクライナ侵攻により、サイバー界でも重大な事件が起きていた。近年最も活発に活動していたランサムウェア攻撃グループ「Conti (コンティ)」の実体が公となり、ソースコードが流出した。また、悪名高いランサムウェア攻撃グループの 1つである「REvil (レビル)」メンバーの一斉逮捕に加え、多数のアンダーグラウンドフォーラムも閉鎖された。それにも関わらず、ダークウェブ (Dark Web) やディープウェブ (Deep Web) を利用した犯罪は、今もなお発生し続けている。こうした市場は、一体どうやって一般ビジネスのような形態を維持しているのだろうか？その理由は、なくなることのない需要と、マーケットの使用性の高さにある。

今回は、ランサムウェア、闇フォーラムおよびサイバー闇市場、そしてハッカーグループを中心に、ダークウェブおよびディープウェブの動向を詳細に紐解いていく。

ダークウェブというと、以前は一部の犯罪者やハッカーだけが利用する空間だと考えられていた。しかし、韓国インターネット振興院 (KISA) によると、ダークウェブへのアクセス者数は 1日平均 1万5千人に達するとされている。

まず初めに、ダークウェブとは一体何を指す言葉だろうか？



[図1] インターネット世界の構造：サーフェイスウェブ（表層 Web）、ディープウェブ（深層 Web）、およびダークウェブ

ダークウェブは、時にディープウェブと混同される場合もあるが、互いに異なる意味を持つ。ディープウェブは、通常の検索エンジンによって収集されない Web ページ全般を意味し、インターネット全体の 96～99% 程度と推定されている。一方のダークウェブは、ディープウェブの最下層に位置する意図的に隠蔽された Web ページを意味し、特定のブラウザを介してのみアクセスすることができる。現在、Web ページ全体の約 5% ほどがこのダークウェブにあたるとされている。

ダークウェブは、その全てが不法行為を目的として利用されているわけではない。しかし、主に悪意を持つランサムウェアグループやハッカーグループに利用されているのが事実だ。

ダークウェブ＆ディープウェブの主な問題点 1：ランサムウェア

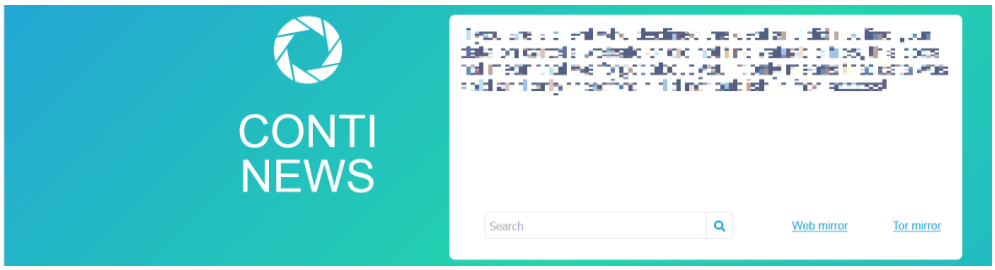
ランサムウェアグループは、絶えずリブランディング（再構築）を続けることで、様々な制裁措置を回避している。最も代表的な例に、ALPHV ランサムウェアが挙げられるだろう。ALPHV、別名 BlackCat と呼ばれるランサムウェアは、同一人物が製作したものと推測される。この製作者は、REvil・DarkSide・BlackMatter・Maze など、複数のランサムウェアグループで活動していたメンバーを積極的に募り、リブランディングを行った。

- リブランディング順序：DarkSide → BlackMatter → BlackCat (ALPHV)

[図2] ALPHV ランサムウェアグループの運営ページ

近年、複数のランサムウェアグループがリブランディングを試みており、そのグループ名が頻繁に変わっている。このことから、実際の彼らの組織形態は、我々が思っているほど大規模ではないとの見方もある。

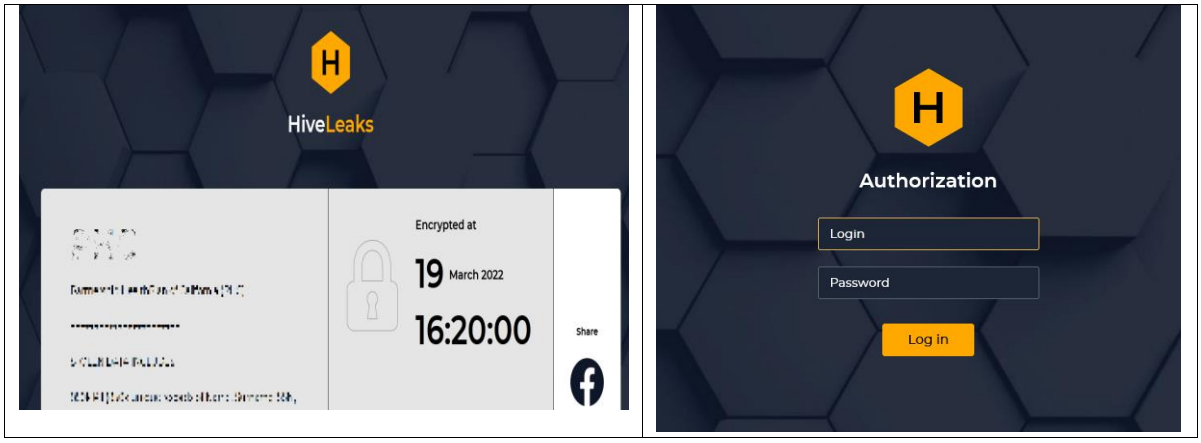
また別の例として、Conti ランサムウェアが挙げられる。彼らは、Ryuk (リューク) ランサムウェアのリブランドとして知られており、その活動は非常に精力的で、これまで 800件を超える組織が Conti ランサムウェアの攻撃を受けている。



[図3] Conti ランサムウェアグループの運営ページ

最近、彼らの会話内容や、ランサムウェアの暗号化・復号化ソースコード、またそのツールなどが流出し始めた。しかし、Conti ランサムウェアグループはそれでもなお活発に活動を続けている。ランサムウェア攻撃をサービスとして提供する RaaS (Ransomware as a Service) は、一般的なビジネスモデルと同じような形態を持っており、こうした内部データの漏洩は、運営する上でさほど大きな影響を及ぼさないことが判明した。

さらに、ランサムウェアの交渉用 Web サイトを別途で運営するランサムウェアグループも増加している。その一例として、 被害者リストのある PR サイトと、交渉用サイトの両方を運営しているのが、下記の Hive ランサムウェアグループである。



[図4] Hive ランサムウェアグループの運営ページ (左)・交渉用ページ (右)

Hive ランサムウェアグループと身代金の支払いを交渉するためには、ランサムノート (身代金要求文書) に記載されている onion アドレスと、ログインアカウント情報が必要になる。彼らはここ最近、基本的な身代金要求額を 120万ドルから 200万ドルに引き上げ、ランサムノートの一部も変更した。

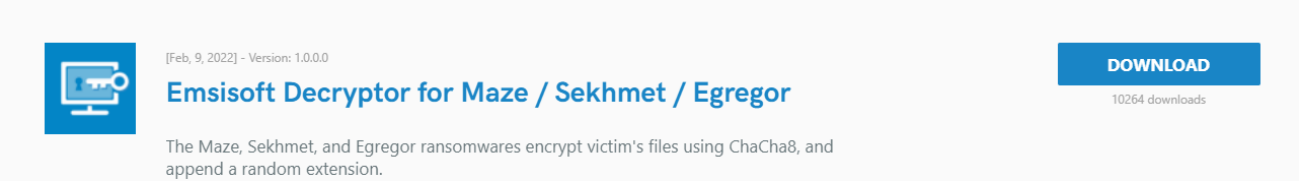
交渉用ページを別途で運営するランサムウェアグループがいる一方で、Linux のような新しい環境で動作するよう変形を加えたランサムウェアグループもいる。LockBit (ロックビット) ランサムウェアグループは、Windows 環境以外にも、Linux や ESXi 環境で動作する変種を保有している。

MD5	V3 診断名
3c9e550d41f3de930e678776a6e018ed	Ransomware/Linux.Generic.260872
9661c01af31a41caef2ccd3b6be06e60	Ransomware/Linux.Generic.259496
18a352d33c8c01b6a196adce176c5a96	Ransomware/Linux.Generic.252680

[表1] LockBit ランサムウェアの Linux 版

LockBit ランサムウェアは、Conti ランサムウェアに匹敵するほどの活発な活動を続けており、ほぼ同等の被害者リストを保有している。被害者リストは 2022年 1月の時点で 500件を超えており、2月中旬には 1度に 14件、3月中旬には 2日間で 22件の新たな被害者がリストに追加された。

精力的な活動を続けるランサムウェアグループとは正反対の動きを見せるケースもあった。突然の解散宣言、または逮捕に至ったグループである。Maze (メイズ) ランサムウェアの製作者と推定される人物は、BleepingComputer.com サイトに Maze (メイズ)、Egregor (エグレゴール)、Sekhmet (セクメト) などのマスターキーを公開した。さらに、この公開された情報をもとに、セキュリティ企業の Emsisoft 社が復号化ツールを製作している。
- URL：https://www.emsisoft.com/ransomware-decryption-tools/maze-sekhmet-egregor?__c=1



[図5] Emsisoft 社の Maze･Sekhmet･Egregor 複合化ツール

Maze ランサムウェアの製作者、またはサイバー闇市場の運営者が解散する理由としては、逮捕、もしくは逮捕への懸念、リブランディング、金銭的目標の達成、健康問題などの個人的な理由があると推測される。

解散を宣言する前に逮捕されたランサムウェアグループもいる。GanbCrab (ガンクラブ) ランサムウェアとして名を馳せ、REvil (レビル)、別名 Sodinokibi (ソディノキビ) にリブランディングしたランサムウェアグループのメンバーは、今年 1月に逮捕されている。

しかし驚くべきことに、このグループは依然として活動を継続していることが確認された。逮捕されたメンバーらは、ペンテスター (pentesters、侵入テストを行う者) もしくはアフィリエイトを担っており、中心人物が逮捕された後も、彼らは新たなグループ名で活動中だという噂もある。

[表2] は、2021年に REvil ランサムウェア関係者が逮捕された時期を時系列で記したものである。

2021年	国および逮捕メンバー
2月、4月、10月	韓国にて REVil および GandCrab 関係者 3人を逮捕
11月	ルーマニア･コンスタンツァにて REVil 関係者 2人を逮捕
11月	クウェートにて GandCrab 関係者 1人を逮捕

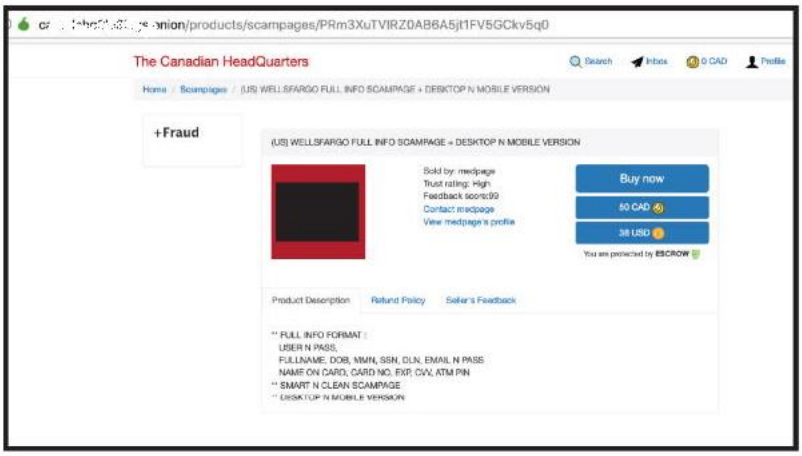
[表2] 時系列でみる 2021年 REvil ランサムウェア関係者の逮捕の流れ

ダークウェブ＆ディープウェブの主な問題点 2：闇フォーラムおよびサイバー闇市場

政府機関が積極的に乗り出したことで、闇フォーラムおよびサイバー闇市場にも多くの変化がもたらされた。政府機関、または法執行機関によって閉鎖されたサイトもあり、自主的な解散、もしくは出口詐欺（Exit Scamming）を敢行したグループもいた。

1. CanadianHQ、Monopoly Market などのサイバー闇市場閉鎖

2018年から運営が続く Canadian HeadQuarters も、カナダ政府によって閉鎖された。CanadianHQ とも呼ばれる Canadian HeadQuarters は、名の通ったダークウェブ闇市場の 1つである。詐欺、薬物、スパム関連サービス、フィッシングキットに加え、奪取した資格情報や、Botnet（ボットネット）に感染したパソコンに関するアクセス情報などが取引されていた。カナダ政府は、このサイバー闇市場の運営者 4人の名前、およびニックネームを公開し罰金を科した。



Screen shot of a stolen Wells Fargo customer's credit card advertised on the Canadian HeadQuarters site. Image from a Terbium Labs report in 2020

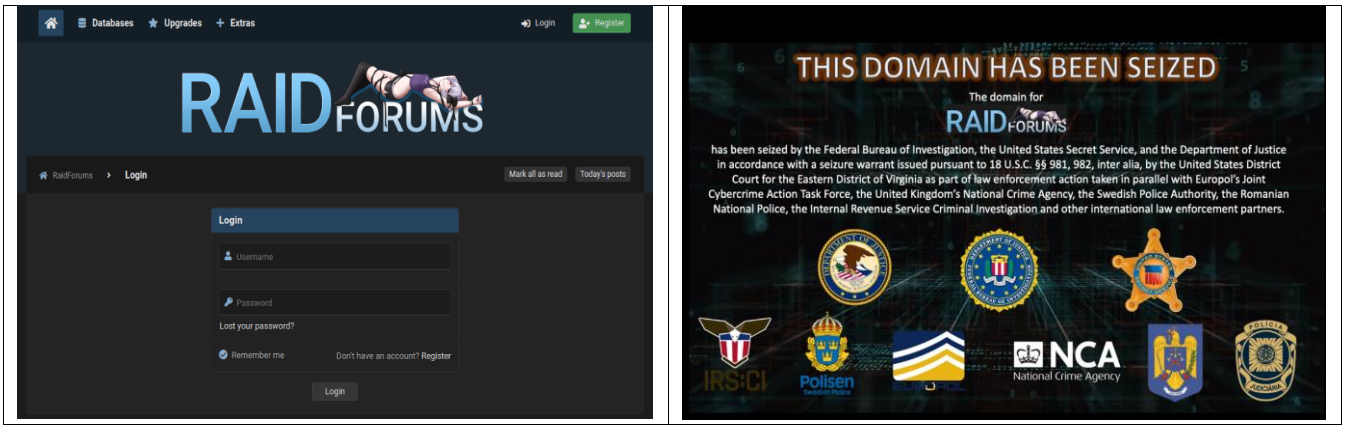
[図6] CandianHQ（出典：Terbium Labs Report in 2020）

2019年に運営が開始された Monopoly Market は、最も運営歴の長いダークウェブ闇市場である。販売商品としては麻薬類が扱われていた。閉鎖の理由は定かではないが、前述の通り、法執行機関による逮捕の懸念、金銭的な目標達成などの理由で、自主的に解散したものと推測される。

[図7] Monopoly Market

2. Raid Forums へのアクセス封鎖

さらに、データベース（DB）の流出経路として広く知られている Raid Forums（レイドフォーラム）に関しては、今年の 2月中旬頃からアクセスできない状態が続いている。Raid Forums は世界最大のハッキングフォーラムの 1つであり、50万人以上のユーザーを保有していた。

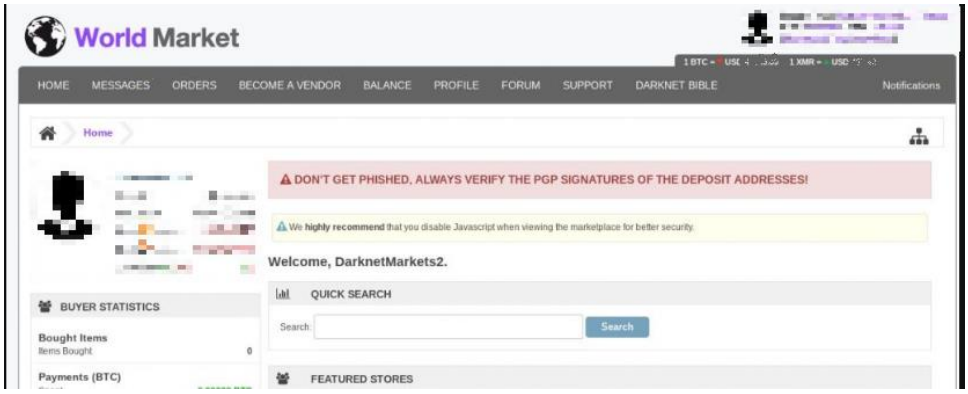


[図8] 閉鎖前の Raid Forums ログインページ (左)、法執行機関によりドメインが押収された現在の様子 (右)

米司法省とイギリス、スウェーデン、ポルトガル、ルーマニアの法執行当局の協力により、現在は [図8] のようにフォーラムが封鎖された状態だ。フォーラムの創立者兼運営者とされる人物は、2022年 4月 12日にイギリスで逮捕された。現在、ドメインは米司法省により押収済みと報じられている。

3. World Market の出口詐欺

2020年 11月から運営が確認されている World Market (ワールドマーケット) は、ここ最近出口詐欺 (Exit Scamming) の問題が取り沙汰されている。World Market はダークウェブ上にある闇市場で、注文が履行されるまでの間資金を保有するエスクロー (escrow、取引保全) サービスを提供している。ところが、最近こうしたサービスにある問題が生じていることがわかった。

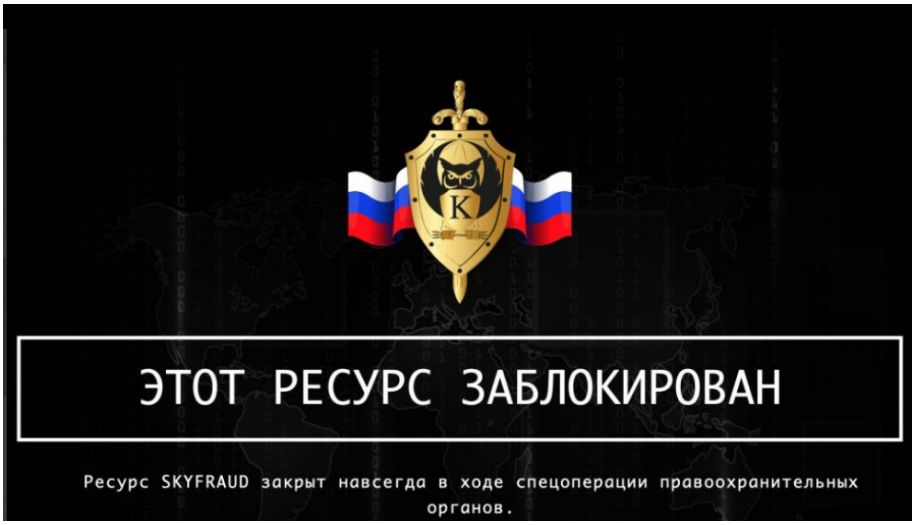


[図9] World Market ログイン後のページ

ユーザーが預けていた仮想通貨の紛失、資金引き出しの遅れ、または少額出金しかできないなどの問題が相次いでいるのだ。

4. SkyFraud および Ferum フォーラムの閉鎖

比較的規模が大きく、奪取したクレジットカード情報の販売を行っていた Sky Fraud および Ferum フォーラム (別名 Carding Forum) も閉鎖へと追い込まれた。



[図10] ロシア連邦内務省・BSTM-K 組織により差し押さえられた SkyFraud のメインページ

この閉鎖は、ロシア連邦内務省の BSTM-K 組織による作戦と推測されている。この作戦で、上記のフォーラム以外にもさらに 2つのフォーラムが閉鎖された。彼らは SkyFraud のメインページに、「次は誰の番か？」というメッセージをロシア語で残し、ロシア内のサイバー犯罪者に対するさらなる逮捕劇を示唆している。

ダークウェブ＆ディープウェブの主な問題点 3：ハッカーグループ

また、闇フォーラムだけでなく、ハッカーグループに関する閉鎖ニュースも相次いだ。2022年 1月、米政府およびブルガリア政府当局の努力により、NetWalker (ネットウォーカー) ランサムウェアグループも閉鎖を余儀なくされた。さらに、アフィリエイト役のカナダ人男性には、80ヶ月もの懲役が言い渡され、彼が所有していた 719.99 BTC (ビットコイン)、15.72 XMR (モネロ) も押収された。

Conti ランサムウェアグループは、ウクライナ在住のセキュリティ研究者により、グループや人物を特定する情報の載ったチャット内容が流出・公開された。公開された内容によると、GOLD BLACKBURN および GOLD ULRICKの 2つのグループが、このランサムウェアグループの主軸であるとされている。

GOLD BLACKBURN は、金銭窃取を目的とするサイバー犯罪グループで、2014年 6月からその活動が確認されている。2016年末から 2022年 3月まで、TrickBot (トリックボット) マルウェアを製作・運営しており、BazarLoader・Anchor・Zloader・Buer Loader などのマルウェアも流布してきた。

2018年半ば頃からその活動が確認されている GOLD ULRICK は、ランサムウェア攻撃専門のグループである。2018年 8月から2021年初めにかけては Ryuk ランサムウェアを流布し、2020年初めからはリブランディングを経た後 Conti ランサムウェアを流布している。

世界中で多くの企業をハッキングした犯罪グループに、LAPSUS$ (ラプサス) というハッカーグループがいる。アクセス管理企業である Okta (オクタ) も彼らにハッキングされ、一部の顧客情報が流出する事件が発生した。この事件は、顧客をサポートする 3rd party 企業の Sykes Enterprises (サイクス・エンタープライズ) が発端となったことが明らかになっている。顧客サポート企業は、顧客からの要求を履行する上で広範囲のアクセス権限を所持しているため、ハッカーグループのターゲットとなるケースが多い。

結論

ディープウェブおよびダークウェブで活動するサイバー犯罪組織は、一般的なビジネスモデルと同じような形態を持つ。こうしたビジネスを維持できる 2つの理由として、途切れることのない需要とマーケットの使用性の高さが挙げられる。

買い手と売り手の距離が物理的に離れたダークウェブ闇市場でも、ランサムウェアは RaaS (Ransomware as a Service、サービスとしてのランサムウェア)、マルウェアは MaaS (Malware as a Service : サービスとしてのマルウェア) を介すことで、そのビジネスは成立する。買い手と売り手をつなぐ中央集中型サービスの提供、ユーザーの等級制度、さらには注文履行までの間資金を保有するエスクローサービスも備えている。こうした使用性の高さ以外にも、高い収益性を誇るため、ディープウェブやダークウェブを悪意のもとに利用するサイバー犯罪者は増え続けている。

ダークウェブやディープウェブ、またそこで活動するサイバー犯罪者を集中的に取り締まるため、国際的な捜査協力が進められている今、彼らの動向や変化は世界的に注視されている。

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)