SECURITY REPORT

2022 APR

CyberFortress

このレポートは、株式会社サイバーフォートレスの独自の調査にて収集されたデータに基づき作成しています。

ハッキンググループその正体は？

01. 概要

DXと共に知能的なサイバー攻撃が急増している。その裏には主要企業と国、有名人などを対象に標的型持続的高度攻撃(Advanced Persistent Threat, APT)を行うハッキンググループが存在する。彼らの目的は様々である。金銭的な利益をとったり、彼らの信念を強くアピールしたり、または社会的な混乱を惹起するために、たまには特定の国に対する諜報行為のために国のサポートを受けながら活動する場合もある。

コンピューターワールドUK(Computerworld UK)によると、ハッキンググループは非公開のカスタマイズツールを活用しており、固有のコマンド及び制御インフラを運用している。高度化された攻撃戦術と技術、方法を基に自分の位置や正体を隠して、犯した罪をまた、他のハッキンググループになすりつけたりする。ハッキンググループは闇の中で密かに活動しているが、サイバーセキュリティ専門家の努力によって一部の情報が明らかにされている。これを基に悪名高いハッキンググループについて調べてみよう。

ハッキンググループその正体は？

02. 北朝鮮のハッキンググループ

まず、必要に応じて部隊を柔軟に構成できサイバー諜報及びテロ遂行、ハッカー育成の世界で最高レベルに到達したと評価される北朝鮮のハッキンググループについて調べてみよう。北朝鮮はハッキングを通じて北朝鮮に影響を及ぼす戦略的な情報を収集することはもちろん国家単位でのお金稼ぎをしているとしられている。

北朝鮮の代表的なハッキンググループで、北朝鮮と関連があると疑われている大体のインシデントに登場する「Lazarus」。Lazarusは2009年、韓国政府と軍のPCに「米軍」、「キーリゾルブ訓練」、「統合参謀本部」などの用語検索で軍事機密を盗みだした「トロイ作戦(Operation Troy)」で、その存在感を表した。2020年にはボーイングなどの主要企業の採用広告に偽装したスピアフィッシング攻撃「ドリームジョブ作戦(Operation Dream Job)」で全世界の数十個所の航空・防衛・企業・機関の侵入に成功した。

ハッキンググループその正体は？

Lazarusは機密情報収集と共に金銭収益目的の攻撃も並行している。2016年発生したバングラデシュの中央銀行ハッキングインシデントはLazarusの配下グループである「Bluenoroff」の仕業だと推定されている。特に最近数年間は仮想通貨の投資企業と取引所を攻撃して北朝鮮が統制しているアドレスに資金を引き抜く攻撃に集中した。シンガポールの仮想通貨取引所であるKuCoinの2億8100万ドル流出事故の背後にはLazarusがいると報道されている。

2017年史上最悪のランサムウェアだと呼ばれる「WannaCry」の攻撃にも関与していると示唆され、その攻撃はユーザーがマルウェアが入っているウェブサイトを訪問したり、メールのマルウェア添付ファイルを実行するように誘導するような、それまでのランサムウェア攻撃とは違った。全世界的に占有率が高いMS WindowsのSMBポートのリモートコード実行脆弱性を活用し、インターネットがつながっている不特定多数のPCや古いOSを使用しているサーバに攻撃することができた。

しかし、この全ての攻撃がLazarusの仕業なのか？セキュリティインテリジェンス企業であるMandiantは「北朝鮮のハッキンググループを指す包括的な用語であり、北朝鮮偵察総局内で遂行されるサイバー作戦として「Lazarus」を理解すべき。」だと説明した。北朝鮮だと疑われる攻撃の戦術、技術、手順(Tactics, Techniques, Procedures, TTPs), 攻撃インフラ、マルウェアなどで類似するところが多いということは攻撃者の間で共有されているリソースがあるという意味でもある。

Mandiantは北朝鮮第1の対外工作機関である総参謀部偵察局(RGB)がほぼすべてのサイバー戦を総括していて、総参謀部偵察局を構成している6つの局の1つ、第3局(海外情報部)傘下の「ラボ110(Lab 110)」は、ハッキンググループ「APT38」、「TEMP Hermit」、そして「Andariel」が中心的存在と分析した。そしてこのハッキンググループ全てが色々な面でLazarusと密接に関連しているとみた。

TEMP Hermitは全世界の国防、通信、金融機関を主要ターゲットとして北朝鮮のための戦略的な情報を収集する。APT38はソーシャルエンジニアリングを使用して主に金融機関に侵入した後、銀行間の通信システムを把握し数千万ドルを引き抜いたとして知られている。悪魔の名前を意味するAndarielは国防人事、防衛産業体、政治組織、エネルギー研究所などを主に攻撃し、最近では政府のための収益確保のために仮想通貨取引所、ATM機器、ギャンブルサイトなどにも活発に攻撃をしているとみられている。

その他にも韓国の水力原子力会社のハッキングの背後で知られている「Kimsuky」は北朝鮮に影響を及ぼす戦略的な情報収集をすることに集中していることで知られている。彼らは日本を含め、アメリカや韓国の政府・軍・製造業界の担当者と学界専門家を主要ターゲットにしている。ターゲットは金融、個人、顧客データの収集から始め、究極的には国家安保、外交政策、学術情報などの情報を獲得することが最終的な目的である。北朝鮮国家安保部がサポートしている秘密情報組織「APT 37」もKimsukyと類似な活動をしている。

ハッキンググループその正体は？

03. ロシアのハッキンググループ

ロシアのハッキンググループも北朝鮮と同等の力を持っていることで有名である。ロシアはソ連国家保安委員会(KGB)後身である連邦保安庁(FSB)にサイバー戦専担部署を置いて、サイバー武器開発と専門家育成に力を入れていると知られている。

まず、ロシア連邦保安庁(FSB)とロシア対外情報庁(SVR)全ての指示を受ける「Cozy Bear, APT29」と「Fancy Bear, APT28」の活動が一番目立っている。 彼らは2016年アメリカの大統領選挙に介入していたと知られている。アメリカの民主党全国委員会(DNS)サーバに侵入し、当時民主党とヒラリー・クリントンとやり取りしていたメールを公開した。Fancy Bearは2008年大統領選挙当時に使用されたメールアドレスに対するフィッシング攻撃を始め、民主党員の最新連絡先を取得し、これを利用し非公開メールアカウントにたいするスピアフィッシング攻撃を行ったとみられている。

ハッキンググループその正体は？

特にFancy Bearはアメリカとヨーロッパを主な標的にし、政府と軍関連機関、政治界、防衛産業体、エネルギー企業、流通企業、メディアなどを狙った全方位的な攻撃を行っていることで知られている。去年７月アメリカ国家安全保障局(NSA)とイギリスの国家サイバーセキュリティセンター(NCSC)はAPT28と同一グループであるロシア連邦軍参謀本部情報総局(GRU)内の特殊組織「GTsSS」が2019年中旬から2021年初めまでにKubernetes clusterを利用してアメリカとグローバル組織を対象に総当たり攻撃を実施し、これに対する警告文を発表したことがある。

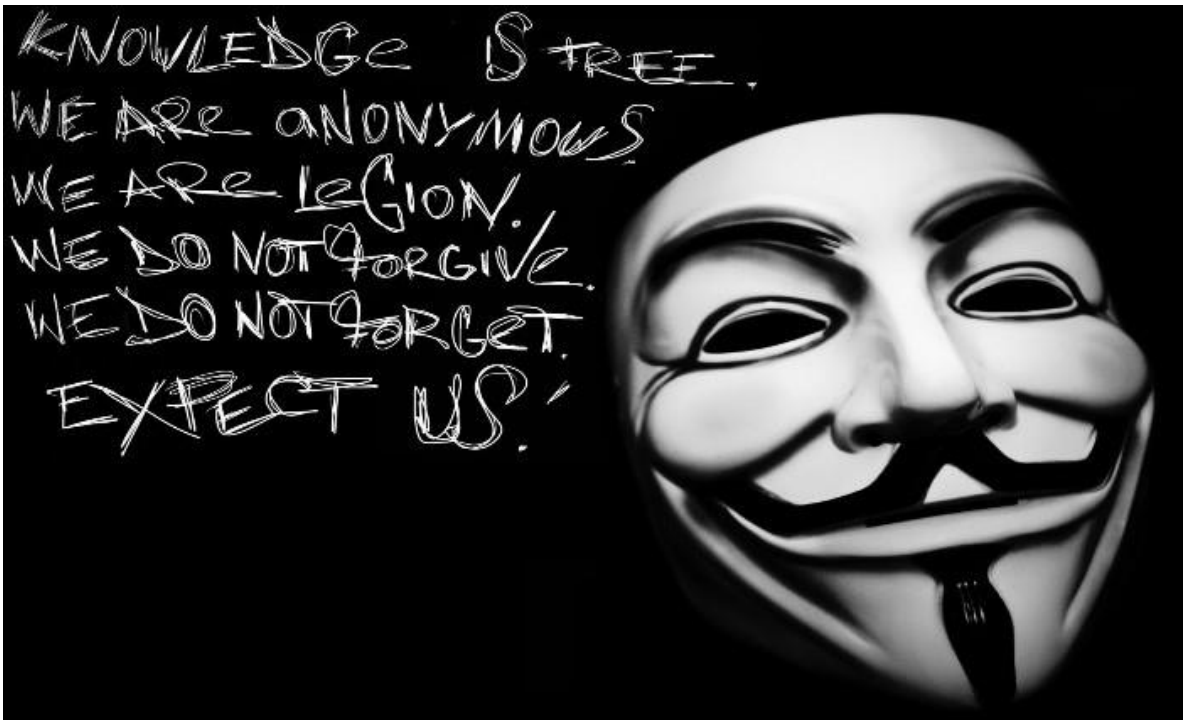
去年の始め、政権が変わったばかりのアメリカ社会に衝撃を与えた「SolarWinds」事態もロシアのハッキンググループが背後にいると知られている。このハッキンググループはSolarWindsサーバにバックドア機能を持っているマルウェアをインストールし、SolarWindsソリューションを使用する約1万8千社から、アップデートの過程でマルウェアを流布した。アメリカ財務省、国務省、国土安全保障省、核武器を担当しているエネルギー省と国家核安全保障局(NNSA)までアメリカの被害はどの国よりも大きかった。アメリカのバイデン大統領はロシア対外情報庁(SVR)の指示を受けるハッキンググループ「Nobelium」の仕業ということを公式に発表し、報復としてロシア外交官を追放した。

2018年韓国を狙って攻撃を試したこともある。平昌冬季オリンピックの運用のための重要システムを狙った「オリンピック破壊者」攻撃である。平昌冬季オリンピック組織委員会とオリンピックインシデント対応チーム(CERT)はオリンピックを狙った攻撃の中で歴代最悪であるこの攻撃を対応し、全世界から注目を浴びた。2020年アメリカの法務省とイギリスの外務省はロシア連邦軍参謀本部情報総局(GRU)のサポートを受ける「Sandworm Team」が長く準備し「オリンピック破壊者」攻撃を行い、これがまるで北朝鮮の仕業のように偽装したと発表した。国際オリンピック委員会(IOC)が不法薬物服用の理由でロシアチームの参加資格を剥奪したことに対する報復だった。

ロシアは物理的な戦争と共にサイバー戦を積極に利用することで有名である。日本時間で今年2月24日ロシアはウクライナへ侵攻し始めたが、サイバー戦はその前から発生したとみられる。ロシアは2014年ウクライナの領土であるクリム半島をロシアの領土に編入しようと、サイバー戦を並行した前歴がある。ロシアからの侵攻の前に行われた4件のロシアと思われる攻撃をロシアは全て否定したが、ウクライナを含め、西欧諸国はロシア政府の支援を受けているハッキンググループの攻撃だと確信している。

ハッキンググループその正体は？

04. アノニマス



(参考：https://blog.naver.com/ninja44486/220551324219)

ロシアとロシア支持組織がウクライナの企業・機関を攻撃している中、これに全世界のハッカーも強く反撃し、サイバー世界大戦が続いている。「アノニマス:匿名」の名前その通りに正体を隠したまま活動し、映画の「Vフォー・ヴェンデッタ」に登場したイギリスの革命家「ガイ・フォークス」の仮面をシンボルとして選んだ「アノニマス(anonymous)」の活動が目立っている。

指導部がない組織であるアノニマスは2000年代の始め、アメリカのコミュニティーサイトの4chan内で作られたとされている。アノニマスの創設以来、収　益ではなく闘争の道具としてハッキングを使用する行動主義者つまり、ハックティビスト(hacktivist：hacking ＋ activist)だと自称し、自身の意見に反する腐敗し、暴力的な国・社会に対してサイバー攻撃を続けている。

アノニマスは2010年暴露専門サイトである「ウィキリークス(WikiLeaks)」を公式的に支持し、ウィキリークスへの寄付金支払いを遮断した複数のクレジットカード会社に分散型サービス拒否攻撃(DDoS)を行い、全世界から高い知名度を持つことになった。当時ウィキリークスはアメリカのニューヨークタイムズ(NYT)とイギリスのガーディアンなどいくつかのメディアに世界各国の指導者に対する赤裸々な評価を含めたアメリカ政府の外交全文25万件を公開したことがある。

ハッキンググループその正体は？

アノニマスは以降にも持続的に自分の意志と対立する国、組織に対する攻撃を続いている。2011年過度な国民情報検閲に反対するアラブ民主化運動が起きると、アノニマスはこれに対する支持を宣言し、チュニジア、エジプトなどの政府サイトを麻痺させた。2015年にはイスラム過激派である「IS」に攻撃を行い、組織員の情報を公開し、計画中のテロの内容明かし追加被害の発生を防いだこともある。去年の始めにはミャンマーの軍部政権に関連するサイトをターゲットにする「オペレーションミャンマー(OpMyanmar)」作戦を行った。

アノニマスは多少異例的に個人に対する大規模な攻撃を予告して話題になった。アノニマスは去年6月、テスラーの最高経営責任者(CEO)の「イーロン・マスク」をターゲットにするYouTube映像を載せた。「数百万名の個人投資家は仮想通貨の収益に依存しているのに、あなたは仮想通貨の相場の騰落をあおって多くの人々の人生を壊している。」というのがその理由だった。アノニマスを成り済ましたハッカーの仕業とうい話も出たが、一方ではアノニマスの影響力は政治、社会を超えて資本まで拡大されたという意味で解析している。

アノニマスは現在ウクライナを侵攻したロシアへの攻撃に集中している。アノニマスはロシアがウクライナを侵攻した直後、ロシア政府に対するサイバー戦争を宣言し、ロシア政府と国営銀行、ロシア光栄メディアなどをターゲットにてして強力なサイバー攻撃を行った。4月初めにはツイッターでウクライナで戦争中のロシア軍人12万名の個人情報を流し、「ウクライナ侵攻に関与したすべての軍人は戦犯裁判を受けざるべきだ」と強調した。

ハッキンググループその正体は？

05. LAPSUS$

LAPSUS$は2021年12月登場した新しいハッキンググループで10代のハッカーで構成されていると推定されている。Nvidiaからマイクロソフトやサムスン電子、LG電子そしてOktaまで自称「LAPSUS$」だと称するハッキンググループから侵害を受けた、もしくは受けたとされるグローバル企業が多くあったことでLAPSUS$は短期間に高い知名度を持つことになった。

LAPSUS$は多国籍の組織員で構成されて、彼らが管理するテレグラムのチャットルームには英語、ロシア語、トルコ語、ドイツ語、ポルトガル語など多様な言語を使う組織員が活動しているとされている。

セキュリティ会社であるSilent PushはNvidiaとサムスン電子のような会社の前にブラジルの保健省、ブラジル及びポルトガルの会社もLAPSUS$の攻撃を受けていたと推定している。3月の始めに発生したヨーロッパのゲーム開発社UbisoftハッキングもLAPSUS$の仕業だとみられている。Ubisoftをハッキングしたというハッカーは現れていないが、LAPSUS$がテレグラムのチャンネルからUbisoftのハッキング記事をお知らせとして投稿し、笑っている絵文字をつけていたということで「自分の行為を認定して広告している」とみられている。

ハッキンググループその正体は？

Digital Shadowsのセキュリティ専門家はLAPSUS$は既存の攻撃者とは大きく二つの部分から明確な方法の違いがあると分析した。まず、LAPSUS$はランサムウェアの代わりにデータを盗んで被害組織を脅迫する戦術をとっている。LAPSUS$はNvidiaとサムスン電子から盗んだデータを流したことに対してはNvidiaをハッキングした後、誰かが逆にLAPSUS$に侵入し盗んだデータを暗号化しようとたからだと言っている。

二番目はLAPSUS$は攻撃後、テレグラムのフォローに攻撃に対するお知らせメッセージを送ったり、被害企業にお金の代わりに変わった脅迫をするなどそのコミュニケーションの方法にも違いがある。例えば、Nvidiaには仮想通貨採掘のためのグラフィック処理装置(GPU)需要爆増を防ぐためにNvidiaがGPUにかけたロックを自ら解いて仮想通貨の採掘にもっとうまく活用できるように要求したことがある。
3月の末、イギリスの警察はLAPSUS$に加担した疑いでLAPSUS$の組織員7名を逮捕し、捜査後、釈放した。しかしLAPSUS$は少しも委縮していなかった。Okta攻撃後、しばらく休暇を取ると言ったLAPSUS$のハッキング組織は最近ルクセンブルクのソフトウェア会社Globantからデータと、資格証明などで構成された70ギガバイトのデータを奪取したと発表し、復帰を知らせた。

KrebsOnSecurityによると、LAPSUS$は緊急データ要請(Emergency Data Request, EDR)など「技術レベルは高くないが、大きい影響を及ぼす攻撃」方法を主に使用していることが確認できた。司法当局の資格証明を盗んだ後、緊急の事案として、通信・インターネットサービス・ソーシャルメディア企業などにデータを即時提供するように誘導する方法である。

また、LAPSUS$は企業の役職員のアカウント情報を収集してエンドポイントにアクセスすることに力をいれている。LAPSUS$はダークウェブでターゲットのシステムにアクセスできる役職員またはサードパーティー職員の情報を購入し、アカウント流出機能があるマルウェアを流布するといった方法で攻撃対象のアカウント情報を収集しているとみられた。Okta事件の場合、LAPSUS$はサードパーティーの御客サポート業者と一緒に働いているエンジニアのノートパソコンからOktaのネットワークに侵入したことが確認できた。

セキュリティ専門かは「一部ではLAPSUS$が子供で構成されている幼稚なハッキンググループだとこき下ろしたりもするが、LAPSUS$の攻撃が非常に効果的であることは否定できない。」としてLAPSUS$の歩みに注意を払うよう示している。