SECURITY REPORT

2022

JUN

ウクライナ・ロシア戦争からみる サイバー戦の動向及び対応方法

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。

ウクライナ・ロシア戦争からみるサイバー戦の動向及び対応方法

01. ウクライナ・ロシア戦争の序幕

2022年2月24日、ロシアのウクライナ侵攻が始まった。今回の侵攻は2014年にウクライナ内にあるロシア自国民保護という名分でロシアがクリム半島を占領し、両国の戦争が始まった。2021年7月ロシアのプーチン大統領はロシア人とウクライナ人は「一つの国民」という見方を強力に披瀝した「ロシア人とウクライナ人の歴史的統合について(Об историческом единстве русских и украинцев)」というエッセーを出版した。その後、これを基調として2022年2月21日ウクライナのドンバス地域に軍隊を配置し、3日後の2月24日ウクライナ向けに全面的な侵攻が開始された。

ウクライナに向けたロシアの物理的な侵攻が始まり、サイバー環境にも変化が確認された。侵攻以前からロシアは技術力、政治力、経済力、軍事力など全ての手段を活用して「ハイブリッド戦争(Hybrid Warfare)」を実施している。ハイブリッド戦争は軍事的な手段を活用する以前の戦争形態に非軍事的な手段の攻撃方法を活用して戦争相手の国の混乱と不安を引き起こす戦争を意味する。最近ではICT技術が飛躍的に発展したことによって、非軍事的な攻撃方法としてサイバーハッキングなどの攻撃が占める割合が高くになり、これはウクライナ・ロシアの戦争でも見ることができる。

サイバー戦争が発生しても一般的に、戦争が行われている国どおしで行われるが、ウクライナ・ロシアの戦争は各国を擁護するハッキンググループが参戦しており、以前の戦争ではなかった独特な形態をしている。ロシアを支持しているハッキンググループの中で、2021年話題になったContiランサムウェア組織は「自分たちはロシア政府を支持し、ロシアにサイバー攻撃を行う誰でも、全ての手段を使って復讐する」といった公式文書を、戦争が始まった直後2月26日に発表した。このようなロシアを支持するハッキンググループに対応するため、ウクライナの副首相ミハイロ・フェドロフはツイッターからウクライナIT軍隊を募集する投稿を記載し、ハクティビストで有名なアノニマスがウクライナを支援するなど多数のハッキンググループがウクライナ・ロシアのサイバー戦に参戦した。

サイバー戦争が国家間の問題を超え、戦争理念に賛同する多数のハッキンググループに拡大し、ウクライナ・ロシアのサイバー戦において「世界大戦」とも呼んでいる。サイバー戦の攻撃形態及び規模によって物理的戦争を超える場合が頻繁にあり、今回のウクライナ・ロシア戦争を基にサイバー戦の影響度とサイバー戦に備える方法について調べてみよう。

02. サイバー戦の概要

1)サイバー戦(Cyber Warfare)の定義

> “ コンピューターネットワークを通じてデジタル化された情報がやり取りされる仮想的な空間に、多様な
> サイバー攻撃手段を使用して敵の情報体系を撹乱、拒否、統制、破壊するなどの攻撃と、これを防御する活動”

サイバー戦はかかる費用に比べ大きな破壊的な効果を誘発するため、政府機関が行うが一般的だが、民間ハッキンググループが行う場合も一部ある。サイバー戦の攻撃は下記のように大きく4つの攻撃形態で分類できる。

IGLOO

1 マルウェアを流布し、ターゲットのコンピューターを麻痺、破壊するシステムへの破壊的攻撃	2 スパイウェア、トロイの木馬をメールで疑われないように送信し、相手のパソコンを感染させて銀行・仮想通貨の口座または、政府・軍事・企業機密情報のような内部主要情報を奪取する情報奪取攻撃
3 メディアにアクセスし、世論を操作し、情報を捏造して人をごまかすなどの心理的な攻撃	4 サービス利用ができないように主要ホームページを麻痺させサービス可用性を低下させる攻撃

このようにサイバー戦はこれまでの戦争形態とは違う形になっている。サイバー戦の特徴は下記の表のようにこれまでの戦争と比べて攻撃が光の速度のように行われる。マルウェアプログラムはミサイルを購入し、発射する費用より安く購入でき、自ら作成・修正できるため、オープンソースを活用して攻撃する場合が多い。また一つの攻撃方法で公共機関、銀行など多数の組織に被害を与えることができ波及範囲が地球的で、密かにに行われる場合が多く、戦時・平時の区分が明確ではない。世界的にコンピューター、サーバの資源や民間ハッカーが活用ができるため、時間と空間の制約はなく、攻撃者が不明確という特徴を持っている。

これまでの戦争	区分	サイバー戦
高費用	準備にかかる費用	低費用
局地的	波及範囲	地球的(広域性)
簡単に把握可能	攻撃者	不明(隠匿、匿名性)
自国資源限定	活用資源	民間及び全世界的な資源活用可能
明確	彼我識別	不明
物理的な限界が存在	攻撃速度	早い
比較的に明確	戦時･平時区分	不明
費用に比例	効果	費用対比効果が克明

【▲ 既存の戦争とサイバー戦の違い (参考：韓国国防研究院、週刊国防論壇 第1431号(12-40))】

ウクライナ・ロシア戦争からみるサイバー戦の動向及び対応方法

2) サイバー戦の現況

＊ 一部の国の場合攻撃事実を否認した場合に限って(推定)で明示

年度	戦争名称	攻撃国	被害国	被害事例
1991	第1次湾岸戦争	アメリカ	イラク	アメリカ国家安保局のコンピューターウィルスの侵入によるイラクの防空網撹乱
1993	コソボ紛争	セルビア	アメリカ	セルビアハッカーがアメリカ軍のネットワークを対象にコンピューターハッキング及びウィルス流布
2006	第2次レバノン戦争	イスラエル	レバノン	レバノン武装勢力ヒズボラ、偽遺体及び爆撃シーンの演出などサイバー心理戦を展開
2007	ロシア・エストニアサイバー戦争	ロシア(推定)	エストニア	エストニアネットワーク攻撃
2008	ロシア・ジョージア戦争	ロシア	ジョージア	DDoS攻撃でジョージア主要機関攻撃及びボットを活用した「メール爆弾」によるネットワーク無力化
2012	イスラエル・パレスチナ紛争	イスラエル	パレスチナ	SNSによるガザ地区空襲友好世論造成
2012	イスラエル・パレスチナ紛争	パレスチナ	イスラエル	パレスチナ武装勢力ハマス、イスラエル軍携帯ハッキング及びサイバー心理戦
2014	ロシアのクリム半島侵攻	ロシア	ウクライナ	サイバー攻撃によるウクライナ大規模停電発生

【▲ サイバー戦の歴史 (参考：「情報・サイバー戦類型と情報技術側面のセキュリティ戦略発展方向」一部再構成)】

サイバー戦は20世紀から21世紀になって頭角を現した。世界人口の中で、インターネットを使用している人の比率が2%にもなっていない20世紀に比べ、21世紀は世界人口の半分以上がインターネットを使うため、サイバー上の影響度が益々大きくなった。上記の表を見ると1991年と1993年に発生したサイバー戦は戦争と直接的に関連する特定の集団に攻撃を試みていたが、2006年以降発生したサイバー戦はメディアを利用したり、ネットワークを攻撃するなど民間にも被害を与えられる心理的な方法に発展した。

過去発生したサイバー戦の中、世界的なセキュリティ専門家が「サイバー戦」と言える最初の事例は2007年エストニアネットワーク攻撃である。公共機関、大統領のウェブサイト、通信、IT企業が標的になり、エストニアに大きいな社会的混乱を与えて、数千万ドルの金銭的な被害が出た。背後にはロシアがいると推定されるが明らかになった情報はなく、背後がいない攻撃だと一旦落ち着いた。その後、ロシアは戦争にサイバー戦を継続的に活用した。2008年ジョージア侵攻時、軍事作戦の前にジョージアの主要機関を無力化させる為ネットワーク、メディア、ポータルまで攻撃した。2014年ロシアのクリム半島侵攻時、ロシア情報組織であるGRUなど正規組織及び民間の有名なハッキンググループを含めて3~5万名ほどのハッカーがウクライナ中西部地域の大規模な停電を発生させた。

このようにサイバー戦は段々と情報撹乱、奪取の領域に発展し、物理的な攻撃もできる形に変化している。現在、戦争を行っているウクライナとロシアのサイバー戦はどのように行っているでしょうか。

3. ウクライナ・ロシアのサイバー戦

1) ウクライナ・ロシアの戦争の様相

ウクライナとロシアがサイバー戦で見せる様相は大きな違いがある。

ウクライナ	区分	ロシア
ウクライナ支持勢力	主体	ロシアハッキング集団 ＋ ロシア支持勢力
公共、通信会社、銀行	対象	公共、通信会社、銀行、メディアなど多方面
DDoS攻撃、ホームページハッキングなど	類型	マルウェア攻撃、ランサムウェア攻撃など
可用性	要素	整合性
短期戦	性格	長期戦
防御	形態	攻撃
サービス利用不可、個人情報収集	目的	システム破壊、心理戦活用、個人情報奪取
支持勢力独自ツール使用	ツール	WhisperGate, AcidRain, Industroyer2, CaddyWiperなどオープンソース使用

【▲ ウクライナ・ロシアサイバー戦の携帯 (参考：イグルーコーポレーション)】

ロシアはロシア情報総局(GRU)とロシア支持勢力が主に攻撃を行い、WhisperGate, AcidRain, Industroyer2, CaddyWiperなどのようなマルウェアを利用して政府、公共機関、通信業者、銀行、メディアなど多方面をに攻撃を試みている。攻撃に使用されるマルウェアを準備する期間は比較的に長いものとみられており、攻撃の目的がシステムを無力化させるなど破壊的な性向と、個人情報収集及び奪取、心理戦の活用など多様な目的で攻撃を試みる形をしている。

一方、ウクライナはウクライナ支持勢力が主に攻撃を行い、公共機関、通信業者、銀行などを攻撃する。ロシアとは異なり特定の対象にサービス拒否攻撃、ホームページハッキングでデータベースを奪取するなどの攻撃をしている。ウクライナの支持勢力はサイバー戦に対する準備期間は比較的短く、サービス拒否攻撃及び内部データを奪取するなど情報収集的な攻撃を行っている。

ロシアの代表支持勢力は「SandWorm」、「FancyBear APT」、「Conti」などがあって、ウクライナの代表支持勢力は国際ハッカー集団「アノニマス(Anonymous)」がある。その他にも各国を支持すると意思を表明したハッカー組織の情報はハッキングに関する情報を扱っているツイッター「CyberKnow」に記載されている。

ウクライナ・ロシア支持勢力がみせる攻撃形態は確実な違いをみせているため、2022年を基準として各支持勢力が行った攻撃に対して調べてみよう。

2) ロシアの攻撃形態

ロシアがウクライナに侵攻する前から発生していた攻撃を目的別に整理する。攻撃の目的は大きく△システム破壊、△サービス利用を制限し、偽情報を送信するなどの心理戦活用、△情報奪取に分けた。

目的 1：システム破壊

＊ 一部の国の場合攻撃事実を否認した場合に限って(推定)で明示

攻撃日付	攻撃概要	ツール	攻撃背後
2022-01-13	ウクライナ情報技術組織に属している機器に 破壊型マルウェアインストール	WhisperGate	ロシア(推定)
2022-02-11	ウクライナ政府機関から送信されたと推定される フィッシングメール多数送信	Cobalt Strike, Grimplant, GrapSteel	UAC-0056
2022-02-23	ウクライナ公用機関にある数百代のコンピューターに データ削除型マルウェア検知	HermeticWiper	ロシア
2022-02-24	ウクライナ政府機関の中でHermeticWiper攻撃を受けていない組織、コードの類似性を共有していない組織に削除型攻撃適用	IssacWiper	ロシア(推定)
2022-02-24	ウクライナ広帯域衛星のインターネットアクセスを妨害する 削除型マルウェア	AcidRain	ロシア
2022-03-17	ウクライナ企業を対象にファイルを削除して感染し システムの特定レジストリを破壊するマルウェア発見	DoubleZero	UAC-0088
2022-04-08	複数のマルウェアを使用するウクライナ変電所攻撃	Industroyer2, CaddyWiper, OPCSHRED, SOLOSHRED, AWFULSHRED	ロシア

【▲ ロシア側のシステム破壊攻撃の形態 (参考： Cyber Peace Institute一部再構成)】

上記の票は2022年を基準にロシアが侵攻を開始する前・後で試みられたシステム破壊を目的とする攻撃を整理した内容で、ロシアを支持する勢力は共通的に「Wiper」マルウェアを主に使用していることが確認できる。Wiperマルウェアは、パソコンに侵入すると保存スペースにあるデータを削除するタイプの不正ソフトウェアを総称する用語で、WhisperGate, HermeticWiper, IssacWiperなどが変造された形で現れた。Wiperマルウェアは損傷されたシステムのファイルにアクセスして修正もできる点からランサムウェアと類似する点があるが、ディスクを暗号化し、復号化と引き換えにお金を要求するランサムウェアとは違い、Wiperマルウェアはディスクのデータを永久に削除する特性をもっている。実際にロシアの支持勢力はウクライナの公共機関、銀行、変電所などを攻撃するなど、システムを破壊する攻撃を長期的に準備して物理的な影響力を与える試みが多数存在した。MSのデジタルセキュリティ部署が作成した分析レポートによるとサイバーハッキング攻撃を試す前後に物理的な攻撃も同時に行っていたと分析されており現在まで全37回のサイバー攻撃が試みられていると発表した。

ウクライナ・ロシア戦争からみるサイバー戦の動向及び対応方法

システム破壊の目的を持っている様々なWiperマルウェアツール5種を紹介する。

1. システム破壊 - ① WhisperGate

2022年1月3日ウクライナの様々な政府機関、非営利団体及び情報技術組織がWhsiperGateというマルウェアで攻撃された。WhisperGateはMBR(Master Boot Record)を削除する削除型マルウェアでランサムウェアに偽装したWiperマルウェアである。この攻撃で政府機関と技術組織から使用しているコンピューターが感染し、攻撃されたコンピューターはオフラインステータスになった。

WhisperGateは2回不正ファイルを流布した後、実行させる。1回目の不正ファイルはユーザーPCのMBRを、ランサムノートを出力するコードに変更させてユーザーがコンピューターを再起動しても立ち上がらず、攻撃者が指定したランサムノートを表示させる。その後、マルウェアは自動再起動を行い、2回目の不正ファイルを実行させる。2回目の不正コードは攻撃者のディスコードチャンネルに追加ペイロードをダウンロードした後実行されファイルを破壊する。WhsiperGateの攻撃は最大に長い時間システムを麻痺させて復旧ができなくすることが目的だと見られる。

1. システム破壊 - ② HermeticWiper

WhisperGateの攻撃に続いて2022年2月24日に主要産業施設に侵入し内部データを削除・破壊する施設破壊型マルウェア、HermeticWiperが発見された。ウクライナの金融、軍需、政府サイトに大規模なDDoS攻撃と共にHermeticWiperを配布した。マルウェアがウィンドウズのドメインコントローラーから直接配布されたため、攻撃者は実行前に長期間アクセスしていた可能性も存在する。HermeticWiperはシステム破壊に重点をおき、復旧ができないようにMBR(Master Boot Record)、MFT(Master File Table)を暗号化・変造して内部データを削除・破壊する特徴を持っている。ロシアはHermeticWiperマルウェア攻撃をされていない組織とコードの類似性を共有していない組織に、他のネットワーク破壊型マルウェアであるIsaacWiper攻撃を実施したとみられる。

【▲ WhisperGateマルウェアの実行流れ(左)、HermeticWiperマルウェアが添付されたメール(右)
(参考： INCA Internet(左)、SOMANSA(右))】

1. システム破壊 - ③ AcidRain

ロシアの侵攻前後でウクライナとその周辺地域に供給されるグローバル・ポジショニング・システム(GPS)と商業用の衛星通信の信号を撹乱させるサイバー攻撃が発生した。アメリカの通信企業のVisasatが運用する通信衛星KA-SATの機能が麻痺されて使用者は2週間以上オフラインで、9,000名ほどのフランスの会員、ヨーロッパの約13,000名とドイツのエネルギー会社が影響を受けた。

攻撃にしようされたツールはAcidRainで装置ファイル名を総括検索し、当該のファイルを根本的に削除する機能を搭載したと知られている。これに対してセキュリティ企業SentinelOneによるとAcidRainを使用した攻撃者は衛星通信装置ファイルシステムやファームウェアに慣れていない、もしくは他の対象に適用しようとする意図を持っていると分析した。またSentinelOneから発見されたファイル名(ukrop)がロシアがウクライナ人を呼称する言葉から由来したと推測されるため、ウクライナに対する攻撃を念頭して開発されたと分析した。

1. システム破壊 - ④ Double Zero

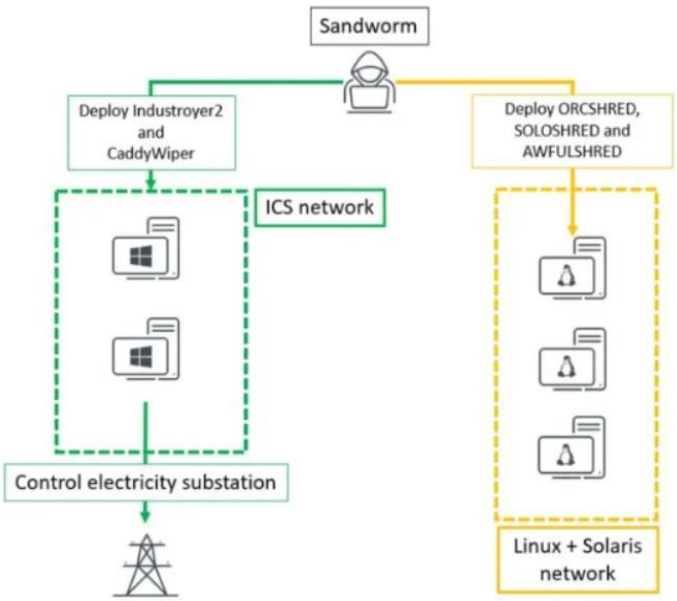
2022年3月23日ウクライナ内の主要機関を対象にしたDouble Zeroという削除型マルウェア攻撃が発生した。セキュリティサービス企業であるESETはDouble Zeroマルウェアが繋がっているドライブからユーザーデータとパーティション情報を削除し、ストレージパーティションを0にして復旧ができないようにさせると分析した。攻撃者は主にスピアフィッシング攻撃で主要機関のPCを感染させた。スピアフィッシングメールは添付されいている圧縮ファイルを解凍するとドットネット(.NET)基盤のプログラムが表示される。当該プログラムはファイルを上書きすることで削除したり、NetFileOpenとNtFsControlFileというAPI呼び出す方法を利用してファイルを削除する。また、HKCU, HKU, HKLM, HKLMのようなレジストリーも削除する。

【▲ ウクライナCERTが発表した「Double Zero」関連レポート (参考：ウクライナCERTツイッター)】

1. システム破壊 - ⑤ Industroye2, CaddyWiper

ロシアのAPTハッキング組織Sandwormがマルウェアでウクライナの変電所を攻撃した。攻撃に使用されたマルウェアは高電圧変電所を無力化させるIndustroyer2とWindows基盤のシステムを無力化させるCaddyWiperでウクライナ変電所のシステム稼働を妨害し、同時にデータを破壊して復旧できないようにさせる。ORCSHRED, SOLOSHRED, AWFULSHREDなど破壊スクリプトを使用してLinux OSを実行するサーバを攻撃した。

ウクライナ政府のコンピュータ緊急対応チーム(CERT-UA)は最初の攻撃が2月から始まって、攻撃の準備期間は最短で2週間前から行われたと分析した。CERT-UAは強力セキュリティ業者である「ESET]で攻撃に使用された産業基盤施設(ICS)不正ソフトウェアは2016年のハッキングで使用されたソースコードと同一のソースコードを利用して設計されたと分析した。今回のハッキングの試みは電力の供給に影響を与えてはいなかったが、もし攻撃に成功していたら約200万人の電力が遮断されたと想定している。



【▲ ロシアAPTハッキング組織Sandwormの攻撃方法 (参考： Security Affairs)】

前に記述した5つの攻撃以外にもロシアの支持勢力はCobalt Strike, Grimplant, GrapSteel, IcedIDなどマルウェアを利用したフィッシングメールの送信及び大量配布でマルウェアダウンロードを誘導し、実行するようにしてデータ及びシステムを破壊する攻撃を続けている。

ウクライナ・ロシア戦争からみるサイバー戦の動向及び対応方法

目的 2：心理戦活用

攻撃日付	攻撃概要	攻撃背後
2022-01-14	ウクライナ政府ウェブサイト約70個にハッキング攻撃発生	UNC1151
2022-01-19	ウクライナ西方政府機関の求職及び雇用サービスのプラットフォームに攻撃試し	APT-Gamaredon
2022-02-15	ウクライナ防衛省、軍隊、大手産業銀行のウェブサイトに大規模DDoS攻撃発生	GRU
2022-02-23	キエフの政府機関及びその他機関の約600個以上のウェブサイトに 最低20個の脆弱性を狙う攻撃試しと数千件のExploit攻撃の発生	中国
2022-02-23	ウクライナ公共機関及び銀行にDDoS攻撃発生	ロシア
2022-02-24	ウクライナ難民の物流を管理する職員を対象にマルウェアが含まれているフィッシングメール送信	UNC1151
2022-02-25	約30個のウクライナ大学ウェブサイトハッキング	theMx0nday
2022-03-09	ウクライナ通信サービス提供業者Triolanが攻撃された全国的に12時間以上ネットワークが中止	不明
2022-03-13	Vinasterriskネットワークに対規模のサイバー攻撃が発生して主要インターネットサービスが中止	不明
2022-03-16	ウクライナ24 TV放送局がハッキングされて虚偽情報を報道し、 大統領が似たようなメッセージを繰り返すディープフェイク映像掲載	不明
2022-03-28	ウクライナ保安局(SBU)から侵攻に関する虚偽ニュースを流すボットファームを識別して処置	ロシア
2022-03-28	UktelecomのITインフラが攻撃されたて13%以下の速度低下発生	不明

【▲ ロシア側の心理的攻撃の形態 (参考： Cyber Peace Institute一部再構成)】

ロシア情報総局(GRU)を含んだロシアの支持勢力はロシアのウクライナ侵攻以降、ある程度の期間をかけ準備したシステム破壊攻撃だけではなく準備期間が短期的なハッキング攻撃で心理的な攻撃が多数試みられている。特にベラルーシ情報部と連携されたハッキング組織UNC1151は侵攻前・後で心理戦を使用する形の攻撃を実施した。

ロシアの支持勢力はウクライナの公共機関、銀行から大学、放送局を攻撃対象として拡大し、対規模のDDoS攻撃を実施してインターネットサービスを麻痺させるなどの行動を見せている。また、上記の表を見ると2022年3月16日に攻撃者はウクライナ24TV放送局をハッキングし、ウクライナの大統領の顔を人工知能を活用した画像合成技術であるディープフェイク(Deepfake)を利用して、虚偽情報をまるで事実のようにニュースとして流してウクライナ国民とその放送を見ている人に混乱を起こそうとしていた。このようにロシア側はサイバー空間を利用して心理的な不安感を助長、世論捏造といった多様な心理的な攻撃を実施している。

ウクライナ・ロシア戦争からみるサイバー戦の動向及び対応方法

【▲ ウクライナ政府機関のウェブサイト攻撃画面 (参考：ロイターツイッター)】

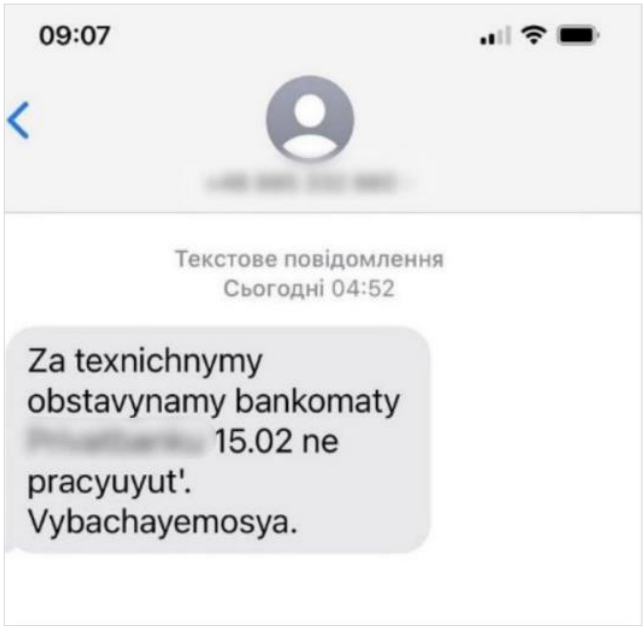
2. 心理戦活用 - ① ウェブサイトの大規模ハッキング

2022年1月14日ロシアのウクライナ侵攻前、ウクライナ政府の約70個ぐらいのウェブサイトに大規模のハッキング攻撃が発生した。上記の図のようにウェブサイトがウクライナ語、ポーランド語及びロシア語などで「恐れよ、最悪を期待しろ。これが君たちの過去であり現在、未来だ。」というメッセージと共に個人情報がインターネットに流出されたという内容が書かれていたが、事実無根だと明らかになった。AP通信はウクライナ問題を論議したロシアと西欧との会談が成果無しで終わり、地域の緊張が高まった状態でハッキングが発生したと伝えた。侵攻前にウクライナ人と周辺国との戦争がすぐ始まりそうな心理的な不安感を助長するためだとみられる。

2. 心理戦活用 - ② 金融系の大規模DDoS攻撃

2022年2月15日ウクライナの防衛庁、軍隊、大手商業銀行(PrivateBank, Oshadbank)ウェブサイトに大規模のDDoS攻撃が行われた。大手商業銀行の場合、使用者の決裁や銀行アプリ使用に問題があったが預託の資金に対する脅威はなかった。専門家はロシアがウクライナの侵攻の前に社会的な混乱を助長するためにウクライナの主要機関にサイバー攻撃を実施する可能性について警告し、実際に攻撃が行われた。ウクライナとロシアの侵攻に対する緊張感を持たせる攻撃だとみられる。

【▲ DDoS攻撃に対するお知らせ (参考：ウクライナ防衛省ツイッター)】



【▲ ウクライナ市民に届いた虚偽メッセージ (参考：ウクライナサイバー警察ウェブサイト)】

2. 心理戦活用 - ③ メディア部分

ウクライナ侵攻以降、ニュース機関に偽装したウェブサイトが、偽の情報を伝えるために展開された。ウクライナ24TV放送局はハッキング攻撃を受け、ウクライナ大統領が戦闘を中断し、武器を捨てることを求めたと虚偽の情報を報道した。ウクライナウェブサイトに大統領が似たようなメッセージを繰り返すなど、ディープフェイク映像を掲載することで虚偽情報を流布した。

2022年3月28日ウクライナ保安局(SBU)は侵攻に関する偽ニュースを広げる100,000個のソーシャルメディアアカウントを動かす5つのボットファーム(Bot Farms)を検知し、閉鎖処置をした。これはウクライナ社会の政治的な状況の不安定化と市民間の恐慌状態を助長するためだとみられている。それだけではなく、DDoS攻撃によりITインフラのネットワーク速度が13%以下に落ちて、軍隊など重要な使用者に対するサービスを中断させない為、ネットワークインフラ保護として個人使用者とビジネス使用者のインターネットアクセスを一時的に制限した。

ロシアはサイバー心理戦を利用して侵攻前後にウクライナ社会を撹乱させて士気を下げるための偽ニュース及び情報を広げる攻撃をしている。戦争への不安感を最大限膨らませ、国民の士気をなくす作戦を共に行っている。

ウクライナ・ロシア戦争からみるサイバー戦の動向及び対応方法

目的 3：情報奪取

攻撃日付	攻撃概要	攻撃背後
2022-02-27	ウクライナ人のアカウントハッキングに成功した対象の ソーシャルメディアのアカウントに利用して虚偽情報掲載	ベラルーシAPTグループ – UNC1151
2022-03-09	被害者を騙して政府から資金をもらうための承認メールを開こうとする Formbook infostealer不成行為発見	不明
2022-03-16	ウクライナ赤十字ウェブサイトを攻撃したが個人データが保存されていないためサイト 情報構成要素のみ影響	不明
2022-03-30	ウクライナ国民及び国内機関にインフォスティーラーMarsStealerの マルウェアが含まれているメールを大量に流布	UAC-0041
2022-04-02	ウクライナ国民を対象にテレグラムアカウントハッキング試し	UAC-0094
2022-04-07	ウクライナメディア組織を対象に物理的な侵攻に対する戦術的支援及び敏感な情報を 盗もうと試していると推定されるインターネットドメイン制御コマンド確認	Strontium
2022-04-14	不正XLS文書を大量に配布してマルウェアを実行させてユーザー資格証明が収集できる バンキングトロイの木馬使用	UAC-0098
2022-04-19	「Ukraine24」を模倣したFacebook詐欺ページから使用者がアンケートに参加するよう にして個人データを調査し、決裁カードデータを損傷させるページに誘導	不明

【▲ ロシア側の情報奪取攻撃の形態 (参考： Cyber Peace Institute一部再構成)】

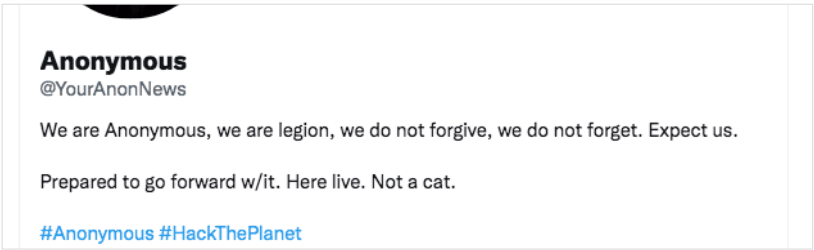
ロシアはウクライナ国民に心理的な影響を与えるため、ウクライナ国民のアカウントを奪取してウクライナ国民に成り済まし虚偽情報を流布する投稿を作成するなどの攻撃を行った。また、個人情報を奪取し、破壊するための攻撃を試みたことも確認した。任意の使用者アカウント情報を奪取して第二次攻撃に使用しようとしたことも確認できた。2月27日は任意の使用者アカウントのハッキングに成功してメディアに虚偽情報を掲載するなど二次攻撃を行って、4月2日にはテレグラムアカウントハッキングを試した。

個人情報を奪取するためのマルウェアを利用した事例も発生した。3月9日に発生したinfostrealer系のマルウェアであるFormbookは主にメールの添付ファイルから流布され、そのファイル名が似ている特徴を持っている。メール本文にマルウェアの流布者のリンクをいれたり、ファイル添付をするなどマルウェアのインストールを誘導して持続的に不正行為を試みて、システム情報とブラウザのログイン情報など使用者の情報を収集する攻撃を実施する。3月30日に発見されたMars Strealerマルウェアは多様なアプリを狙い、広範囲な情報奪取機能を搭載し、47個以上のダークネットサイトとハッキングフォーラム、テレグラムチャンネル、クラックパックのような「非公式」経路から配布されている。

そのほかにも持続的にウクライナ国民を対象にする個人情報及び金融情報奪取行為が続いており、企業を対象に企業情報の漏洩を狙う攻撃も続いている。主に侵攻以前から使用していたマルウェアを利用して攻撃を行っているとみられている。

3) ウクライナの攻撃形態

ウクライナのサイバー戦攻撃の形態はロシアに比べ防御的な性質を見せている。ウクライナ紛争が始まってから外部に表面化したサイバー攻撃の中で一番目立つ攻撃を実施した集団は、断然アノニマス(Anonymous)である。



【▲ アノニマスのハッキング攻撃参戦ツイッター内容 (参考 : YourAnonNewsツイッター)】

2月26日アノニマスがロシア国営TVチャンネルをハッキングしてウクライナから行っている戦争の事実を放送した投稿をアノニマスソーシャルメディアのアカウントから共有した。続けてロシアエネルギー企業Gazprom、国営メディアRTなどのサイトをダウンさせることに成功しクレムリン公式サイトとロシア政府機関及び同盟国であるベラルーシ政府関連サイトも攻撃した。また、ベラルーシ武器生産業者Tetradrのメールの200GBぐらいを流出させ、ロシアのガス供給システムを管理するTvingo Telecomシステムを麻痺させた。アノニマスが使用した攻撃方法に関してサイバーセキュリティ会社Red Goatのパートナであるリサ・フォルテは「今までのハッキング攻撃は大体基本的なレベルであった。」と言った。これでロシア支持勢力に比べてウクライナの支持勢力の攻撃は比較的に準備期間が短く攻撃方法が簡単であると確認される。

04. 最後に

ウクライナ・ロシアのサイバー戦はもう両国だけではなく世界の各国に拡大する可能性が高まっている。アメリカのジョー・バイデン大統領は3月21日(現地時刻)最高経営者分岐会議「ビジネスラウンドテーブル」から「ロシア政府がサイバー攻撃を行う可能性があるという情報を手に入れた。」と明らかにした。アメリカはロシアのサイバー攻撃があれば反撃すると警告しており、サイバー世界大戦の可能性は高まっているとみられている。またサイバー戦に対応するためには主要インフラに対する攻撃を阻止し、民間企業にサイバーセキュリティを強化するための努力を促した。

また、サイバー戦に関して企業は攻撃に備えシステムの脆弱性を持続的に確認し、脆弱性は直ぐに対応し、攻撃モニタリングで被害を最少化する努力が必要である。企業だけではなく個人もサイバー戦に対するセキュリティ認識を高め、フィッシングメールやマルウェアダウンロードなどの脅威に備えるべきである。戦争はもはや物理的な空間だけではないことを自覚する必要がある。

05. 参考資料

1) https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/
2) https://www.msspalert.com/cybersecurity-news/ukraine-russia-cyberattack-timeline-updates-amid-russia-invasion/3/
3) https://www.csoonline.com/article/3655976/new-threat-group-underscores-mounting-concerns-over-russian-cyber-threats.html
4) https://www.asaninst.org/contents/%ED%95%98%EC%9D%B4%EB%B8%8C%EB%A6%AC%EB%93%9C-%EC%A0%84%EC%9F%81%EC%9D%98-%EC%9C%84%ED%98%91%EA%B3%BC-%EB%8C%80%EC%9D%91/
5) https://www.weforum.org/agenda/2022/03/how-the-cyber-world-can-support-ukraine/
6) https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=citrain64&logNo=100170093253
7) https://hemiliar.tistory.com/486
8) https://www.boannews.com/media/view.asp?idx=104223
9) http://koreascience.or.kr/article/CFKO201423965828097.pdf
10) http://blog.skby.net/%EC%82%AC%EC%9D%B4%EB%B2%84%EC%A0%84-cyber-warfare/