NTT Security Holdings

ウクライナ侵攻とランサムウェア動向

NTTセキュリティ・ジャパン
OSINTモニタリングチーム
2022年6月24日

暴露型/二重脅迫型ランサムウェアについて

NTT Security Holdings

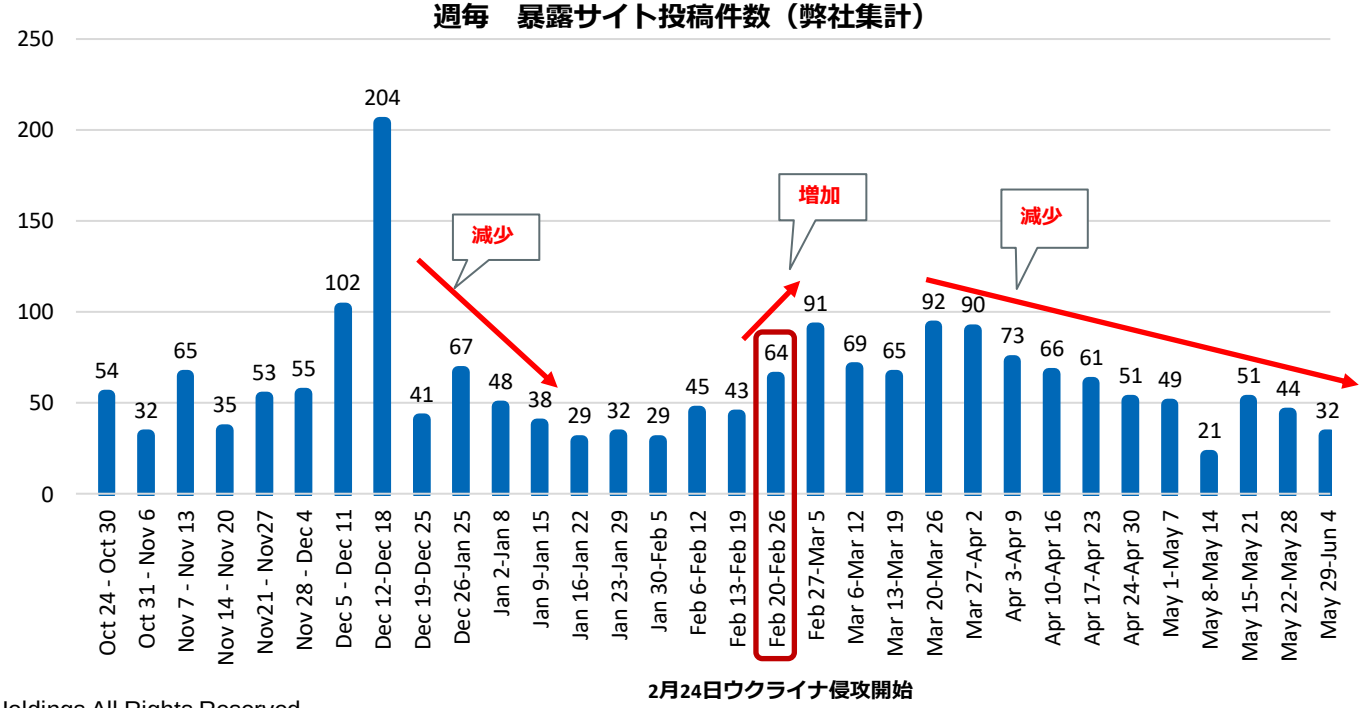
- ランサムウェア攻撃はデータを暗号化して身代金を要求する。それに加えて2019年頃より、暗号化前に窃取したデータの暴露を盾に身代金を要求する二重脅迫と呼ばれる手法が現れるようになった。

- データの暴露はダークウェブに設置された暴露サイトで行われており、弊社ではこれらの監視を行っている。暴露サイトを設置するランサムウェアグループは新旧の出入りが激しいが、40サイト前後がアクティブな状況である。

- グループの多くはロシア語話者によって運営されており、それらは主に西側諸国の組織を標的としている。これを裏付けるようにCIS（旧ソ連諸国で構成する独立国家共同体）諸国の組織は、ほとんど被害に遭っていない。

暴露サイト投稿件数のトレンド

- 暴露サイトでの投稿数は昨年12月まで増加傾向であったが、年明け以降、乱高下を繰り返し、これまでとは異なるトレンドを見せている。
- ロシアのウクライナ侵攻に関わる国際情勢の変化がランサムウェアグループの活動に影響を与えている可能性が考えられる。



ウクライナ侵攻前夜　～減少～

- 2022年1月、ロシア連邦保安庁がランサムウェアグループ REvil のメンバーら14名を逮捕した。ロシアが自国を拠点とする主要なランサムウェア犯罪活動を取り締まるのは、これが初めてであった。
- このことは、ロシアを攻撃しなければ逮捕されることはない、という不文律のルールの元に活動を行っていた犯罪者に衝撃を与え、サイバー犯罪者の掲示板では恐怖や不安を感じるハッカー達の投稿が相次いだ。
- ロシアは米国の要請に応えて逮捕したことを明言しており、ウクライナ侵攻前夜の米国との緊張が高まっているタイミングでの逮捕について、妥協点を探る外交取引を狙った可能性が指摘されている。

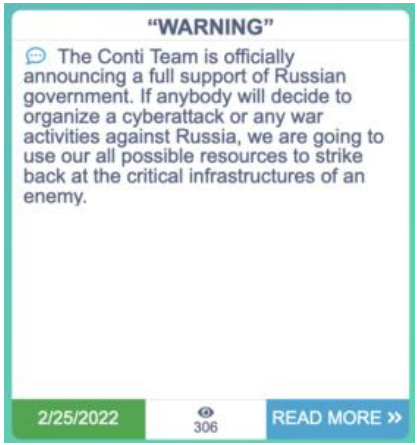
Revil　逮捕時の様子

出典：
https://www.cyberscoop.com/sky-fraud-takedown-russia-cybercrime/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/dark-web-recon-cybercriminals-fear-more-law-enforcement-action-in-the-wake-of-the-revil-takedown/
https://www.youtube.com/watch?v=OqEWuFmzhzs

ウクライナ侵攻直後　～増加～

- ロシアによるウクライナ侵攻は、西側諸国への攻撃を行ってもロシア政府から逮捕される恐れがない状況に変化したことを意味し、怯えていたランサムウェアグループに安心と刺激を与えた。
- Free Civilianランサムウェアグループは、侵攻直後にウクライナの政府機関（gov.uaドメイン）などから窃取したというウクライナ市民の個人情報を暴露サイトで数多く公開し、ロシアのサイバー攻撃の一翼を担った。
- 侵攻開始の翌日、Contiランサムウェアグループは自身の暴露サイトにて「ロシア政府を全面的に支持することを公式に宣言する。ロシアの活動を妨害する者に対しては反撃を行う。」と発表した。
- 4月には、ロシア政府に1月に逮捕されていたはずのREvilが活動を再開した。

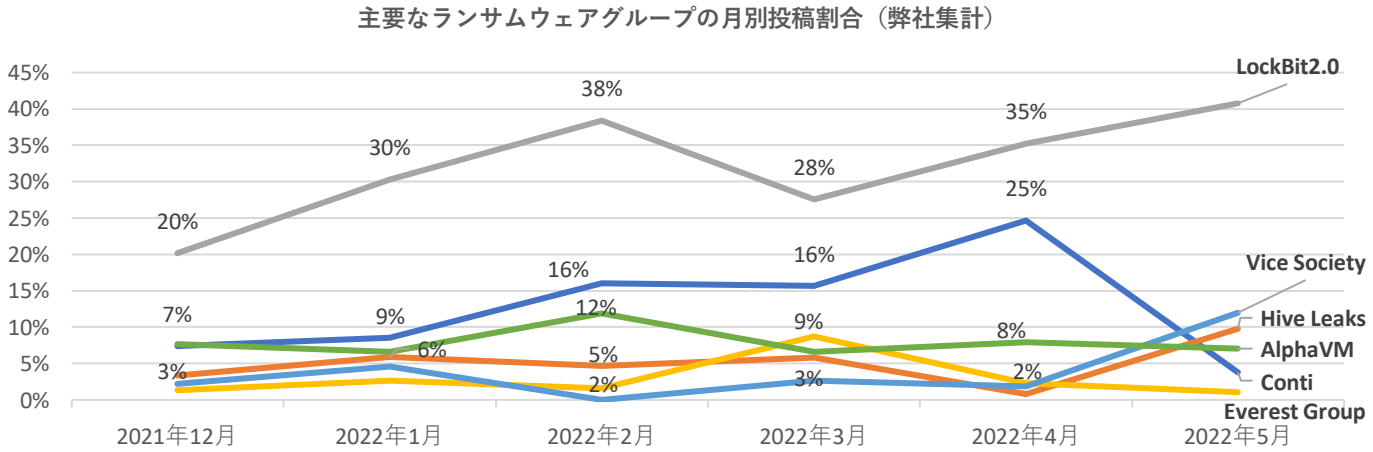
Free Civilianの暴露サイト



Contiはロシア政府を支持することを宣言

Conti Leaks

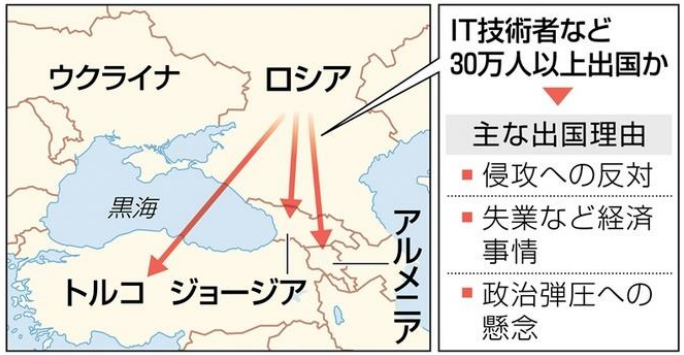
- Contiのロシア支持の宣言に反発し、 2月28日、ウクライナのあるセキュリティ研究者がTwitterアカウントを介してConti内部の数年間のチャットログを漏洩させた。
- このチャットログからは、ロシア政府との関係性や、 Contiの犯罪者集団としての内実（職種ごとに月給制で働いており、実態は一般企業とほとんど変わりないこと、離職率が高く、常に優秀な人材の確保に苦労していることなど）を垣間見ることができる。
- 漏洩後もContiには引き続き勢いが見られたが、 5月になると急に衰えた。西側諸国による対ロシア制裁への抵触の恐れやロシアへの忌避感から、前述の宣言からロシア政府との結びつきがみられるContiへの身代金要求に応じる企業が減少した為とみられている。



出典：https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape

4月以降　～減少～

- ロシアの思惑とは異なり、ウクライナ侵攻は短期間で決着しなかった。経済制裁の影響で多くの外国企業がロシアから急激に距離を置くようになり、事業を存続させるために海外に移転を余儀なくされるハイテク企業も出てきた。
- 経済制裁の影響に加えて、言論統制や徴兵のリスクを避けるために、膨大な数のIT技術者がロシアから流出していることが報じられた。
- ロシア電子通信協会は3月下旬、5万～7万人のIT技術者が国を去り、さらに4月までに最大17万人が出国すると推計した。
- ランサムウェアグループの実態はほとんどIT企業と変わりないことから、ロシアという国家の求心力の低下に加え、IT技術者の国外流出が、4月以降のランサムウェア活動の緩やかな減少に影響している可能性が考えられる。



ロシアの「頭脳流出」先と出国理由

出典：
https://apnews.com/article/russia-ukraine-putin-immigration-kazakhstan-technology-c041eb0b7472668087bb94207de2f71d
https://www.nishinippon.co.jp/item/o/919331/

免責事項

- ランサムウェアグループはグループ名を変更することがありますが、本資料ではグループの変遷は追わず、サイト毎に集計を行っております。
- 本資料における暴露サイトの投稿数は弊社が確認できたものを集計したもので、実際の投稿数と異なる場合があります。
- 本記事の内容は、正確であることに最善を尽くしておりますが、内容を保証するものではなく、本記事の利用に起因して発生したいかなる損害、損失についても補償しませんのでご留意ください。

Security Holdings