令和５年９月 27 日
警　　察　　庁
内閣サイバーセキュリティセンター

中国を背景とするサイバー攻撃グループ BlackTech によるサイバー攻撃について（注意喚起）

警察庁及び内閣サイバーセキュリティセンターは、米国家安全保障局（NSA）、米連邦捜査局（FBI）及び米国土安全保障省サイバーセキュリティ・インフラ庁（CISA）とともに、下記の中国を背景とするサイバー攻撃グループ「BlackTech」（ブラックテック）によるサイバー攻撃に関する合同の注意喚起を発出しました。

注意喚起：People's Republic of China-Linked Cyber Actors Hide in Router Firmware

BlackTech は、2010 年頃から日本を含む東アジアと米国の政府、産業、技術、メディア、エレクトロニクス及び電気通信分野を標的とし、情報窃取を目的としたサイバー攻撃を行っていることが確認されています。

この注意喚起は、BlackTech によるサイバー攻撃の手口を公表することで、標的となる組織や事業者に、直面するサイバー空間の脅威を認識いただくとともに、サイバー攻撃の被害拡大を防止するための適切なセキュリティ対策を講じていただくことを目的としております。あわせて、ネットワークの不審な通信を検知した際には、速やかに所管省庁、警察、セキュリティ関係機関等に情報提供いただきますようお願いします。

なお、注意喚起に示した BlackTech の手口及び対処例の主な内容は、以下のとおりとなります。

【初期侵入】

BlackTech は、インターネットに接続されたネットワーク機器に対し、ソフトウェアの脆弱性を狙うほか、ネットワークの設定の不十分さ、サポートの切れた機器・ソフトウェアなど、標的ネットワークの様々な脆弱な点をサイバー攻撃することにより侵入します。

【海外子会社からの侵入】

BlackTech は、最初の足がかりとなる侵害拠点を構築すると、侵害活動を拡大させるため、海外子会社の拠点において、本社との接続のために使用される小型のルーターを、攻撃者の通信を中継するインフラとして利用します。このように BlackTech は、信頼された内部のルーターを通じて、本社や別の拠点のネットワークへ侵入を拡大することが確認されています。

特に複数の拠点を有するネットワークの管理に携わる事業者においては、サイバー攻撃が常にインターネット側から行われるとは限らず、既に侵害された組織内部のネットワークから攻撃が行われ得ることを念頭に置いていただき、自組織だけでなく関連するグループ組織、システムの開発・保守業者等と連携して対策を講ずることが必要です。

【ルーターの侵害手口】

BlackTech は、様々なメーカーのネットワーク機器を侵害するために脆弱性を調査していると考えられます。BlackTech は、稼働中のシスコ社製ルーターのファームウェアを、改変されたファームウェアに取替えることが確認されています。改変されたファームウェアに取替えることにより、BlackTech 自身の悪意あるサイバー活動のログを隠蔽（いぺい）し、より長期にわたり、標的ネットワークへのアクセスを維持することが目的と考えられます。

【リスク低減のための対処例】

対処例の主な内容は、次のとおりです。注意喚起本文もあわせて参照の上、サイバー攻撃を検知し、自組織のネットワークを守るための緩和策を講じていただくようお願いします。

○ セキュリティパッチ管理の適切な実施

ソフトウェアや機器の脆弱性に対して、迅速にセキュリティパッチを適用する。パッチ適用を可能な限り迅速化し、適用漏れをなくすため、脆弱性管理やパッチ管理を行うプログラムの導入を検討する。

○ 端末の保護（いわゆるエンドポイント・プロテクション等）

端末（PC、タブレット端末、スマートフォン等）のセキュリティ機能の活用や、セキュリティ対策ソフトの導入を行う。

○ ソフトウェア等の適切な管理・運用、ネットワーク・セグメンテーション

ソフトウェア及び機器のリストを管理し、不要と判断するものは排除する。また役割等に基づいてネットワークを分割する。

○ 本人認証の強化、多要素認証の実装

パスワードスプレー攻撃やブルートフォース攻撃によって認証が破られるリスクを低減するために、パスワードは十分に長く複雑なものを設定する。また、複数の機器やサービスで使い回さない。システム管理者等においては、多要素認証を導入し本人認証をより強化する。また、不正アクセスを早期に検知できるようにするために、ログイン試行を監視する。

○ アカウント等の権限の適切な管理・運用

アカウントやサービスの権限は、そのアカウント等を必要とする業務担当者にのみ付与する。特権アカウント等の管理・運用には特に留意する。

○ 侵害の継続的な監視

ネットワーク内で不審な活動が行われていないか継続的に監視を行う。たとえば、業務担当者以外がシステムやネットワークの構成に関する資料へアクセスするといった通常の行動から外れた活動や、外部の様々な脅威情報と一致するような不審な活動の監視を行う。

○ インシデント対応計画、システム復旧計画の作成等

インシデント発生時に迅速な対応をとることができるように、インシデント対応の手順や関係各所との連絡方法等を記した対応計画を予め作成し、随時見直しや演習を行う。また包括的な事業継続計画の一部としてシステム復旧計画の作成等を行う。

○ ゼロトラストモデルに基づく対策

境界防御の効果が期待できない場合を踏まえた認証等の強化を図るとともに、インシデントの予兆を把握した段階で即時に検知と対処ができるような仕組みや体制を整備する。

【参考資料】

○「People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices」（令和４年６月 10 日公表　NSA, FBI, CISA）

https://media.defense.gov/2022/Jun/07/2003013376/-1/-1/0/CSA_PRC_SPONSORED_CYBER_ACTORS_EXPLOIT_NETWORK_PROVIDERS_DEVICES_TLPWHITE.PDF

○「People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection」（令和５年５月 24 日公表　NSA, FBI, CISA 等）

https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_PRC_State_Sponsored_Cyber_Living_off_the_Land_v1.1.PDF

○　「NETWORK INFRASTRUCTURE SECURITY GUIDE」（令和４年６月 22 日公表　NSA）

https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF

○　「PERFORMING OUT OF BAND NETWORK MANAGEMENT」（令和２年９月 11 日公表　NSA）

https://media.defense.gov/2020/Sep/17/2002499616/-1/-1/0/PERFORMING_OUT_OF_BAND_NETWORK_MANAGEMENT20200911.PDF

○　「Attackers Continue to Target Legacy Devices」（令和２年 10 月 19 日公開　Cisco Systems ブログ）

https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954

○「家庭用ルーターの不正利用に関する注意喚起について」（令和５年３月 28 日公開　警視庁）

https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/notes/router.html

○「サイバーセキュリティ経営ガイドラインと支援ツール」（令和５年５月 31 日公開　経済産業省）

https://www.meti.go.jp/policy/netsecurity/mng_guide.html

（以上）