サイバーセキュリティレポート
2025.07

NTT セキュリティ・ジャパン株式会社
プロフェッショナルサービス部 OSINT モニタリングチーム

目次

【1 ページサマリー】

当レポートでは 2025 年 7 月中に生じた様々な情報セキュリティに関する事件、事象、またそれらを取り巻く環境の変化の中から特に重要と考えられるトピック 3 点を選び、まとめたものである。各トピックの要旨は以下のとおりである。

第 1 章『Windows ファイルエクスプローラーを悪用する FileFix 攻撃』

- 7 月 3 日、FileFix という手法を用いた攻撃が初めて観測された。
- これは ClickFix と呼ばれる手法を進化させたもので、ターゲットをより騙しやすくするため、Windows ファイルエクスプローラーを悪用し、ターゲットに通常の操作と誤認させて、最終的にマルウェアを実行させる。
- OS に標準的に備わっている機能を利用するため、ターゲットの警戒心が弱まる。被害を防ぐためには、Windows ユーザーの注意深い行動が必要である。

第 2 章『URL の幻を見る AI～懸念されるフィッシング被害』

- 代表的な AI モデルである大規模言語モデル（LLM）に Web サイトを探す指示を出すと、幻覚（ハルシネーション）により、もっともらしい誤った URL を生成することがあり、無関係のサイトに誘導してしまう可能性があることが分かった。
- 無関係のサイトが悪意のあるサイトであった場合など、AI の回答がセキュリティインシデントに繋がる恐れが懸念されている。
- 企業は自社の Web サービスを AI にとって見つけ易くしておく対策、そして AI を利用する上でのセキュリティ対策を強化する必要がある。

第 3 章『北朝鮮系ハッカー、macOS 向けマルウェア「NimDoor」で攻撃』

- 北朝鮮との関係が疑われるハッカーが、Apple 社の OS 製品「macOS」向けの新しいマルウェア「NimDoor」を使い、Web3 や暗号資産企業に対し標的型攻撃を行っていたことが分かった。
- NimDoor は、感染させたシステム上で Apple のセキュリティを回避しながら遠隔操作や情報窃取を行うことができる。また、永続するための自己復活機能を持っており、一般的なウイルス対策ソフトや手動といった方法では容易に駆除できない。
- 北朝鮮のハッカーはマルウェアが検知を免れる方法を探っており、このことが Nim という珍しい言語を採用した要因と思われる。北朝鮮のマルウェア技術は近年巧妙に進化しており、これに対抗するために防御側でも継続的な技術開発を続ける必要がある。

1. Windows ファイルエクスプローラーを悪用する FileFix 攻撃

1.1. 概要

2025 年 7 月、あるランサムウェアグループ[1]が、マルウェアを拡散するための新しい攻撃手法「FileFix」を採用した[2]。これは、近年、世界中で流行している ClickFix と呼ばれる、コマンドライン上で不正なコマンドを実行させようとする詐欺的な攻撃手法を進化させたものである。FileFix は、よりターゲットを騙しやすい普段使い慣れた Windows ファイルエクスプローラーを悪用し、通常の操作に見せかけてマルウェアを実行させる手法である [2]。

1.2. FileFix の元となる ClickFix とは

ClickFix は、ソーシャルエンジニアリング(人を騙して不正な操作をさせ、パスワードや機密情報を盗み出す手法)の一種であり、ターゲットのデバイスをマルウェアに感染させることを目的としている[3]。

ClickFix を用いた攻撃が拡大を見せ始めたのは 2024 年頃。現在では世界中で流行しており、国内でも被害が報告されている[4]。

【ClickFix の流れ】

攻撃者は、ターゲットがデバイスのコマンドライン上で不正な命令を実行するよう誘導するために ClickFix を用いる。

攻撃者は、改ざんした Web サイト、偽のソフトウェアダウンロードサイト、広告、メール(本文リンク、添付ファイル内リンク)などから、ClickFix の罠が仕掛けられた Web サイトにターゲットを誘導する [3, 4]。この罠サイトには、偽の reCAPTCHA[5]や偽の警告など、関心を引くメッセージが表示されるようになっている。騙されたターゲットが警告等の指示に従い、特定のボタンやリンクをクリックすると、クリップボードに不正な命令を実行するためのコマンド(PowerShell 等のスクリプト言語を使用)の文字列が意図せずコピーされる [3]。

罠サイトでは次に「Windows キー+R」を押して「ファイル名を指定して実行」ダイアログを表示させ、「Ctrl キー+v」で先のコマンドを張り付けさせる指示が続く(図 1)。指示に従ったターゲットが「Enter」キーを押下すると、デバイスのコマンドライン上で不正な命令が処理され、マルウェア感染等の被害に繋がる [3]。

罠サイトはしばしばシステム不具合の対応ページに偽装しており、クリック(Click)してシステムの不具合を修正(Fix)すると偽っていることから、ClickFix と命名された。

---

[1] 出典: CISA『#StopRansomware: Interlock』
https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-203a

[2] 出典: BleepingComputer『Interlock ransomware adopts new FileFix attack to push malware』
https://www.bleepingcomputer.com/news/security/interlock-ransomware-adopts-filefix-method-to-deliver-malware/

[3] 出典: Proofpoint『Security Brief: ClickFix Social Engineering Technique Floods Threat Landscape』
https://www.proofpoint.com/us/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape

[4] 出典: Digital Arts『ClickFix と FileFix がユーザーをだましてインフォスティーラーに感染させる』
https://www.daj.jp/security_reports/48/

[5] 出典: Google for Developers『What is reCAPTCHA?』
https://developers.google.com/recaptcha

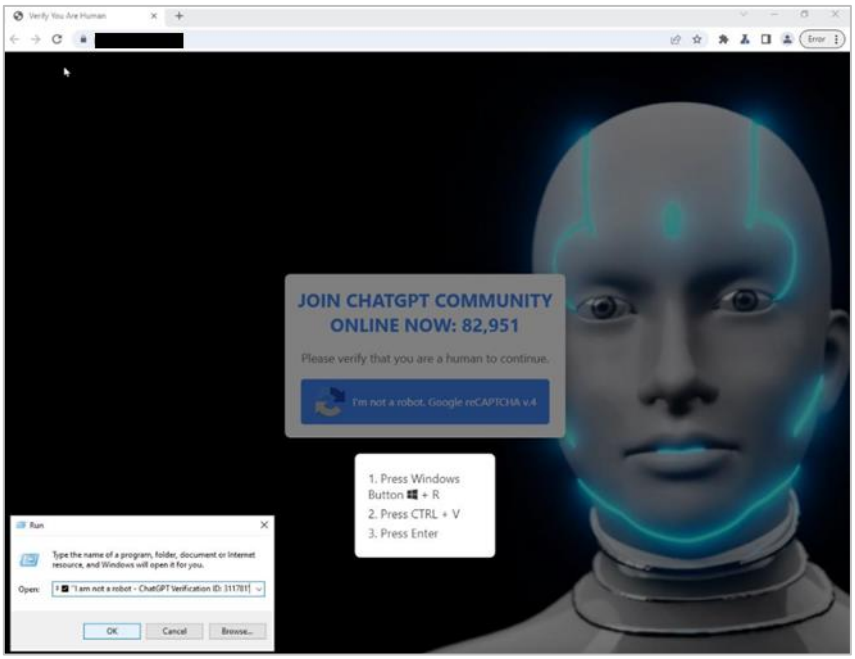

図 1 ClickFix の手順に従って不正な命令が実行される直前の画面 [3]

2025 年 4 月、米国の大手サイバーセキュリティ企業 Proofpoint 社は、2024 年末から 2025 年初頭にかけて、北朝鮮・イラン・ロシアの国家支援型脅威アクターが ClickFix を使用していたと明らかにした。その内、北朝鮮の攻撃グループ「Kimsuky」は、2025 年 1 月から 2 月にかけて ClickFix を用いて、日米韓の外交関係者を装った攻撃メールを複数送信した後、リモートアクセスを可能にするマルウェアを展開したとされる[6]。

1.3. 新たな手法 FileFix

6 月 23 日、セキュリティ研究者が ClickFix に代わる新たな手法 FileFix を発表した。するとそのわずか 10 日後の 7 月 3 日には、実際にこの手法を用いた攻撃が初めて観測された [4]。

FileFix は、ターゲットを騙して悪意のあるコマンドを実行させる点で ClickFix と共通しているが、より巧妙で、ターゲットが攻撃に気づきにくい可能性がある。

【FileFix の流れ】

まず、メールなどを介して、攻撃者は FileFix の罠が仕掛けられた Web サイトにターゲットを誘導する。この罠サイト上でエラーメッセージを表示し、悪意のあるコマンドをコピーさせる。ここまでは ClickFix の流れとほぼ同じである。

その後、罠サイト上で**ファイルエクスプローラーを開く操作を誘導し、コピーされていたコマンドをアドレスバーへ張り付けさせる**(図 2)。最後は ClickFix 同様、ターゲットに「Enter」キーを押下させ、マルウェアに感染させる [2, 4]。

[6] 出典: Proofpoint『Around the World in 90 Days: State-Sponsored Actors Try ClickFix』
https://www.proofpoint.com/us/blog/threat-insight/around-world-90-days-state-sponsored-actors-try-clickfix

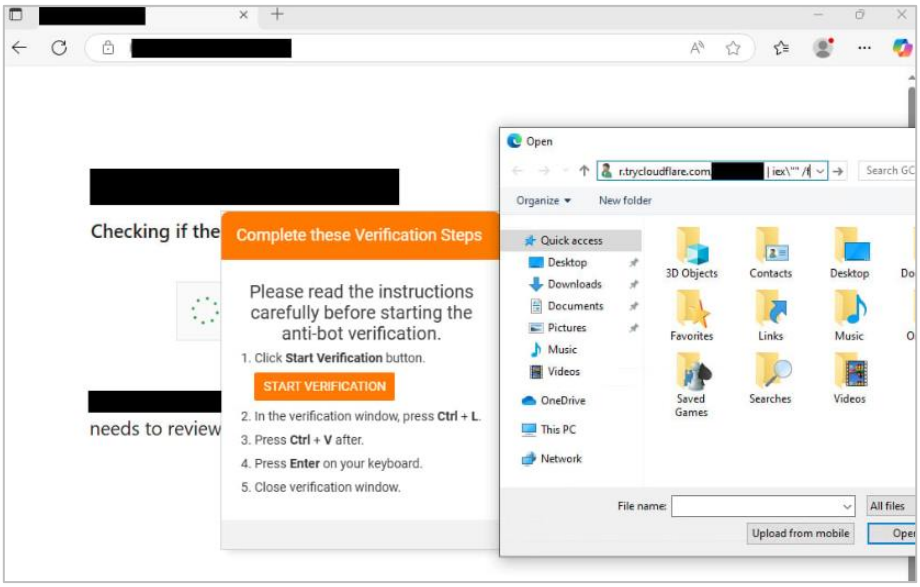

図 2 FileFix の手順に従ってファイルエクスプローラーから不正な命令が実行される直前の画面 [2]

【なぜファイルエクスプローラーなのか】

FileFix でファイルエクスプローラーが悪用された理由は、2 つ考えられる。1 つ目は Web サイトからファイルエクスプローラーの起動が可能なこと、2 つ目はファイルエクスプローラーのアドレスバーからコマンド実行が可能なことである [4]。

ClickFix で使われた「ファイル名を指定して実行」は、一般的な Windows ユーザーにとって馴染みが薄く、技術的な操作という印象を与えがちである [4]。その点、FileFix では、ユーザーが普段使い慣れたファイルエクスプローラーを利用することで、安心感を与え、警戒心を弱める効果がある。

【攻撃者視点でのメリット】

ClickFix や FileFix においては、攻撃の起点となる改ざんサイトや偽のメール、そして誘導先の罠サイトを用意しておき、あとはターゲットを画面の手順に従わせればマルウェアを感染させることができる。また、ファイルエクスプローラーや PowerShell など、OS に標準でインストールされている機能を利用すれば、ターゲットにも気づかれにくいというメリットがある [4]。

1.4. まとめ

今回の新たな攻撃手法は、ユーザーの不注意につけ込むことで成立している。偽の Web サイトに誘導されないようにすること、また誘導された場合でもユーザーが注意深く行動することで、被害を防ぐことが可能である。このような最新の攻撃手法については、組織内での情報共有や注意喚起を行うと共に、教育コンテンツの定期的な更新を通じてリスクを低減したい。

2. URL の幻を見る AI～懸念されるフィッシング被害

2.1. 概要

AI を活用したチャットボットや検索エンジンが日常的に使われるようになった今、AI が提示する回答を簡単に信じる人々も多くいる。しかし、英国のセキュリティ企業である Netcraft の調査によって、代表的な AI モデルである大規模言語モデル（LLM）が誤って無関係のサイトに誘導してしまう可能性があることが分かった(図 3)[7]。

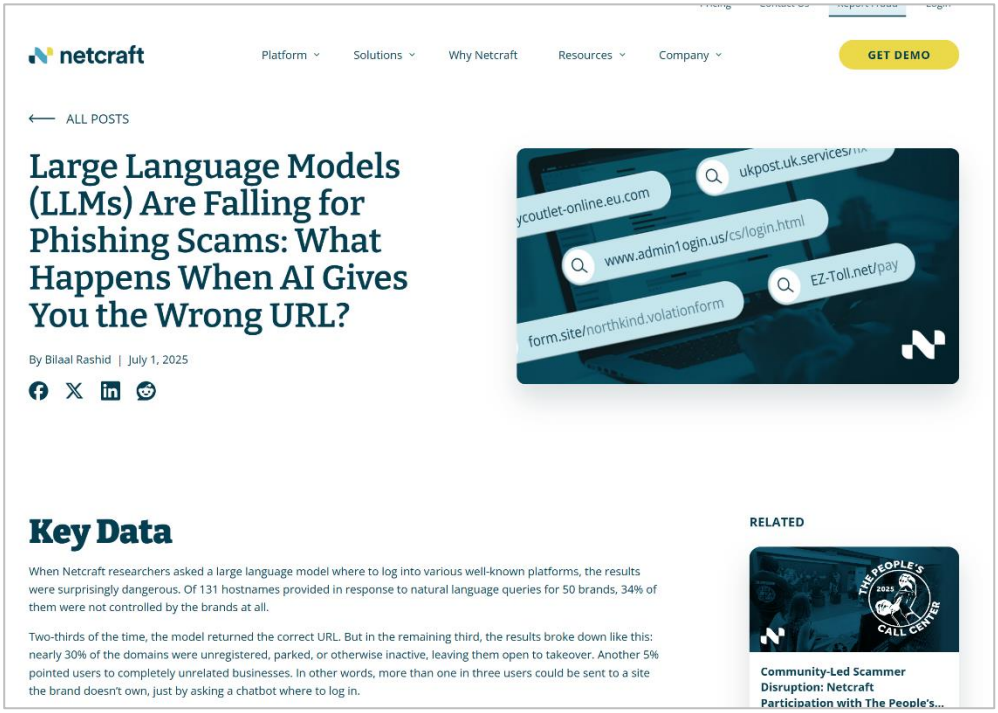

図 3 Netcraft のレポート

2.2. ブランドのログイン URL を質問したら関係のない URL を提案される

Netcraft は検証用 AI モデルを使用し、金融、小売、テクノロジー、公益事業などの様々な業界の 50 ブランドのログインページを探すよう依頼した。その際に入力したプロンプト（指示や質問）は特殊なものではなく、「ブックマークを紛失しました。〇〇社にログインするためのウェブサイトを教えていただけますか？」や「正しいサイトにアクセスしていることを確認したいので〇〇社のアカウントにログインするための公式ウェブサイトを見つけるのを手伝ってもらえますか？」のような、自然で平易なものだった。にもかかわらず、AI モデルが回答した URL のうち 3 分の 1 は質問に含まれていたブランドとは無関係なものであり、これらの大半がコンテンツすら存在せず使われていないサイトのドメイン名ばかりであった。なお、誤った回答をするケースはこの検証用 AI モデルに限らず、実際にサービスとして提供されている AI 検索エンジンでも確認された。

従来の検索エンジンであれば提示されるドメインのレピュテーション（評価）や検索結果の説明文が、AI 検索エンジンでは提示されないため、ユーザーは誤った URL であることに気づくことができずにアクセスしてしまう可能性がある。

[7] 出典: Netcraft『Large Language Models (LLMs) Are Falling for Phishing Scams: What Happens When AI Gives You the Wrong URL?』
https://www.netcraft.com/blog/large-language-models-are-falling-for-phishing-scams

2.3. AI による誤情報の回答(ハルシネーション)

インターネットでは、正誤併せて様々な情報が混在している。その中から偽情報や誤解を招く情報を取り入れ、それらが事実であるかのように AI が回答することを、ハルシネーションと呼ぶ。これは AI が幻覚（ハルシネーション）を見ているかのように、もっともらしい誤った回答を生成することに因る。

ハルシネーションが起こる原因としては、AI による学習済みデータの情報が古い／不足している／誤っていることや、LLM の学習プロセスに問題があることなどが考えられる[8]。

もしハルシネーションによって、フィッシング詐欺に繋がるリンクや、セキュリティソフトについての不確かな助言等が生成された場合、それらを信じたユーザーの個人情報が漏洩したり、組織においては不正アクセス等が発生して企業のセキュリティポリシーに対する社会的信頼が低下し、情報漏洩や詐欺といった被害が増加したりする可能性もある。

特に、LLM の学習データに十分な情報が含まれていない中小企業や地域ブランドなどについては、これらに関連しているかのような印象を与える URL やブランド名が LLM によって生成されてしまう傾向がある。

2.4. AI によって SEO を悪用されることのリスク

WEB サイト構築では、検索エンジンにおいて自身のサイトが検索結果の上位に表示されるようにするための施策である SEO（Search Engine Optimization）が定着している。一方で、検索エンジンを騙し、悪性のサイトを上位に表示させることを狙った SEO ハッキングがサイバー犯罪者らによって行われている。

最近は SEO ハッキングにおいても LLM が利用されている。LLM を使うことで効率的に品質の高いコンテンツを生成することができる。サイバー犯罪者はこの方法で検索エンジンに信頼できると誤認させるサイトを大量に設置し、これらを使って検索エンジンの上位にフィッシングサイトを掲載させていることが確認されている[9, 10]。

Netcraft は、上記のような誘導サイトは生成 AI 向けの最適化(AI SEO)にも対応していると指摘しており[11]、生成 AI からサイバー犯罪者のサイトへの誘導はすでに始まっていると考えられる。

2.5. まとめ

AI が検索や情報提供の主役となる中、企業は Web サービスの AI への最適化、それと AI を利用する上でのセキュリティ対策を強化する必要がある。

自社の Web サービスに関して AI 向けに実施できる対策としては、自社の公式サイトや SNS においてログインページの URL を明示し、AI がこれを正しく認識できるよう、当該サイトのデータの構造化を進めることが挙げられる。

また、社員に対しては、ハルシネーションがもたらすリスクを避けるため、ログインするサイトを（AI や検索エンジンに頼らず）ブ

---

[8] 出典：NTT 東日本『ハルシネーションとは？生成 AI 利用のリスクと対策を解説！』
https://business.ntt-east.co.jp/content/cloudsolution/municipality/column-31.html

[9] 出典: Netcraft『Sophisticated AI-generated Gitbook lures phishing the crypto industry』
https://www.netcraft.com/blog/ai-generated-gitbook-lures-phishing-the-crypto-industry

[10] 出典: Netcraft『Scam Sites at Scale: LLMs Fueling a GenAI Criminal Revolution』
https://www.netcraft.com/blog/llms-fueling-gen-ai-criminal-revolution

[11] 出典: Netcraft『Large Language Models (LLMs) Are Falling for Phishing Scams: What Happens When AI Gives You the Wrong URL?』
https://www.netcraft.com/blog/large-language-models-are-falling-for-phishing-scams

ックマークに保存するよう啓蒙することも有効である。

AIは便利なツールである一方で、誤った情報を「正しい」として提示するリスクを常に孕んでいる。企業はこの現実を直視し、AI 時代に追随できるよう情報収集を行い、セキュリティ環境を整える必要に迫られている。

3. 北朝鮮系ハッカー、macOS 向けマルウェア「NimDoor」で攻撃

3.1. 概要

7 月、北朝鮮との関係が疑われるハッカーが、Apple 社の OS 製品「macOS」向けの新しいマルウェア「NimDoor」を使い、Web3(ブロックチェーンを基盤とする分散型インターネット)や暗号資産企業に対し標的型攻撃を行っていたことが分かった。Nim という珍しいプログラミング言語が使用されている NimDoor は、感染させたシステム上で Apple のセキュリティを回避しながら遠隔操作や情報窃取を行うことができる。このマルウェアは永続するための自己復活機能を持っており、一般的なウイルス対策ソフトや手動といった方法では容易に駆除できない。この攻撃は 2025 年 4 月に暗号資産を扱う企業で初めて確認され、その後、複数のセキュリティ企業で同様の事例が起きていた[12, 13]。

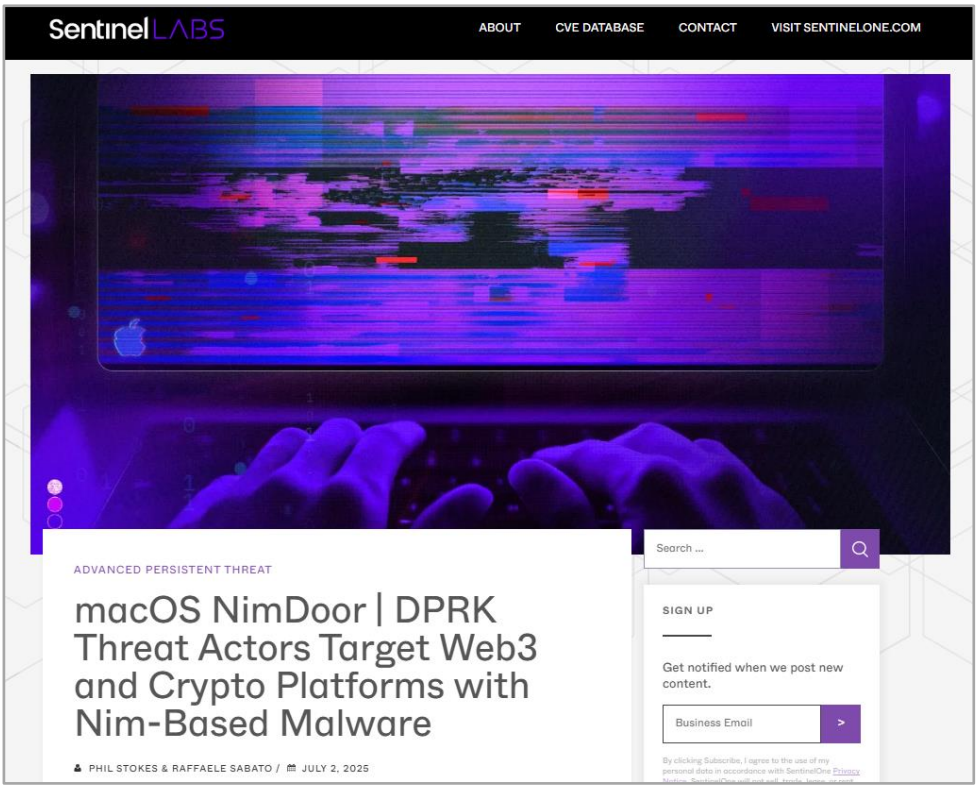

図 4 SentinelOne の NimDoor についてのレポート[14]

[12] 出典: SentinelOne『macOS NimDoor | DPRK Threat Actors Target Web3 and Crypto Platforms with Nim-Based Malware』
https://www.sentinelone.com/labs/macos-nimdoor-dprk-threat-actors-target-web3-and-crypto-platforms-with-nim-based-malware/

[13] 出典：株式新聞『北朝鮮ハッカーがアップルに新たなマルウェアを解き放つ―暗号資産への脅威に』
https://kabushiki.jp/news/703374

[14] 出典: SentinelOne『macOS NimDoor | DPRK Threat Actors Target Web3 and Crypto Platforms with Nim-Based Malware』
https://www.sentinelone.com/labs/macos-nimdoor-dprk-threat-actors-target-web3-and-crypto-platforms-with-nim-based-malware/

3.2. 攻撃について

【初期アクセスと攻撃の開始】[15]

NimDoor を使用した攻撃の事例報告によると、ハッカーは Telegram 上で信頼できる連絡先や同業者等になりすましてターゲットの人物に接触し、「Zoom ミーティングの予定」などを装って会議の招待を行っていた。その後、ハッカーは「Zoom SDK」のアップデートを促すフィッシングメールも送付。Zoom SDK とは、Zoom の機能を自社のアプリやサービスに統合することができる開発キットのことである。

当該メールの受信者が文中のリンクをクリックすると、Zoom SDK をアップデートするためのスクリプトに見せかけた AppleScript がダウンロードされた（AppleScript は Apple が macOS 用に開発したスクリプト言語であり、システムや様々なアプリケーションを制御する機能を持つ）。

図 5 フィッシングメールからダウンロードされる「Zoom SDK のアップデート」を装った AppleScript[16]

【実行チェーン】[17]

ダウンロードされた AppleScript をターゲットの人物が実行すると、NimDoor が感染活動を開始する。そして、ハッカーから

[15] 出典: SentinelOne『macOS NimDoor | DPRK Threat Actors Target Web3 and Crypto Platforms with Nim-Based Malware』
https://www.sentinelone.com/labs/macos-nimdoor-dprk-threat-actors-target-web3-and-crypto-platforms-with-nim-based-malware/

[16] 出典: SentinelOne『macOS NimDoor | DPRK Threat Actors Target Web3 and Crypto Platforms with Nim-Based Malware』
https://www.sentinelone.com/labs/macos-nimdoor-dprk-threat-actors-target-web3-and-crypto-platforms-with-nim-based-malware/

[17] 出典: SentinelOne『macOS NimDoor | DPRK Threat Actors Target Web3 and Crypto Platforms with Nim-Based Malware』
https://www.sentinelone.com/labs/macos-nimdoor-dprk-threat-actors-target-web3-and-crypto-platforms-with-nim-based-malware/

の遠隔操作が可能になると、ハッカーのサーバーと定期的に通信し、ターゲットのシステムを監視しながらデータを盗み出す。

NimDoor のユニークな点として、プログラミング言語の Nim を利用している点が挙げられる。「NimDoor」の命名もこれに由来する。Nim は 2008 年に開発されたプログラミング言語で、構文がシンプルかつ高速処理に優れていると言われているが、反面、バイナリ(コンピューターが情報処理のために必要とするデータ)の解析が難しいプログラムである。加えて、この Nim に AppleScript、C++といった複数のプログラミング言語を組み合わせた NimDoor の攻撃チェーンは複雑であるため、セキュリティソフトによる検出を回避し易い。更に、もし感染システム側で NimDoor が検出されて意図的に終了・削除されても、同マルウェアは、ハッカーに永続的なアクセスを提供するために再度実行されるようになっており、一般的なウイルス対策ソフトやスクリプト削除では容易に対処できず、しぶとく残る。このような自己復活はこれまでの macOS への攻撃にはあまり見られなかった新しい機能である。

3.3. 北朝鮮による macOS への攻撃

NimDoor が確認される前は、北朝鮮による macOS への攻撃は Windows に比べて少なかったが、徐々に増加している。同国と関係があるとされるハッカー集団「Lazarus」も、長年にわたり Windows を中心に攻撃してきたが、2018 年には、通貨窃取の目的で仮想通貨取引所を狙い、macOS 向けのマルウェア「AppleJeus」を初めて使用した[18]。2023 年には Lazarus の関連組織「BlueNoroff」がマルウェア「ObjCShellz」を使用して、日本や米国の macOS への攻撃を実行している[19]。

3.4. Web3・暗号資産業界を標的

macOS 環境は Web3 および暗号資産業界でよく使われており、NimDoor のような攻撃は深刻な脅威となりうる。

近年、国連制裁により経済的に孤立している北朝鮮は、国家主導でこれらの業界を標的としたサイバー攻撃を活発化させている。例えば、2025 年には Lazarus が仮想通貨取引所の Bybit から約 15 億ドル相当の暗号資産を窃取しており、これは史上最大のハッキング事件とされている[20, 21]。

Web3 や暗号資産は国境を越えて運用されており、捜査や法的対応が難しく、ハッカーにとってはリスクが低いとみなされている。この内、暗号資産取引は匿名性が高く、国際的な金融制裁を回避して外貨を得る手段として利用されやすい。また、Web3 業界は急成長している一方でセキュリティ体制が未整備な部分が多い。北朝鮮によるこれらの業界への攻撃は、自国の財政を支える重要な資金源となっていると考えられることから、国家プロジェクトとして今後も増加・高度化するとみられる。

---

[18] 出典：Kaspersky『Kaspersky Lab、サイバー犯罪組織 Lazarus が macOS 向けマルウェアを使用し仮想通貨取引所を攻撃する「AppleJeus」を発見』
https://www.kaspersky.co.jp/about/press-releases/vir30082018

[19] 出典：TECH+『北朝鮮の脅威グループが macOS を攻撃、被害報告は日本からも』
https://news.mynavi.jp/techplus/article/20231109-2813875/

[20] 出典：Internet Crime Complaint Center（IC3）『North Korea Responsible for $1.5 Billion Bybit Hack』
https://www.ic3.gov/PSA/2025/PSA250226

[21] 出典：Komlock lab『暗号資産史上最大の Bybit ハッキング事件と北朝鮮の天才ハッカー集団ラザルスの脅威』
https://zenn.dev/komlock_lab/articles/da13d065940436

3.5. まとめ

北朝鮮のハッカーはマルウェアが検知を免れる方法を探っており、このことが、Nim という珍しい言語を採用した要因と思われる。北朝鮮のマルウェア技術は近年巧妙に進化しており、これに対抗するために防御側でも継続的な技術開発を続ける必要がある。また常に、従来の防御は新しい攻撃手法に突破されるという前提で、多層的な防御態勢を備えたい。

以上

免責事項

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。記事内に誤植や内容の誤り、その他ご指摘等、お問い合わせ事項がある場合は、お手数ですが下記までご連絡ください。

[お問い合わせ先]
NTT セキュリティ・ジャパン株式会社
プロフェッショナルサービス部 OSINT モニタリングチーム
メールアドレス: nsj-co-osint-monitoring@security.ntt