サイバーセキュリティレポート
2025.09

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 9 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『Salesforce の顧客企業を狙った機密情報窃取』

- アプリケーションの Salesloft Drift やソーシャルエンジニアリングを利用した攻撃が多数確認されており、Salesforce の顧客企業から大量のデータが窃取されている。
- 事件に関与しているとみられる攻撃グループは、窃取したデータを公開するとして Salesforce に対して身代金を要求しているが、同社は応じない方針を表明している。
- Drift を介して行われたようなサプライチェーン攻撃は、今後も攻撃者の関心を集めるであろうことに留意が必要である。

第 2 章『新たなランサムウェア攻撃手法 ～AI による著作権侵害～』

- 新たなランサムウェアグループ「LunaLock」が、窃取したアート作品を AI モデルの学習データセットに提供するという新しい脅迫手法を用いた攻撃活動を展開している。
- AI に一度学習されたデータは削除が困難で半永久的に残るため、AI の出力を通じて著作権等の権利侵害が繰り返し発生する恐れがある。
- 今回の事件は、デジタル化が進む現代において、人間の独創性が生かされるべき分野が直面する新たな脅威を浮き彫りにしており、AI 企業側での対策が急がれる。

第 3 章『中国発 AI ペネトレーションテストツール「Villager」』

- AI を活用したペネトレーションテストツール「Villager」(ヴィレジャー)のダウンロード数が、リリースから 2 か月後の 9 月時点で 1 万回を超えた。このツールは、中国拠点のグループ「Cyberspike」が開発している。
- Villager を利用すれば、専門知識がなくても高度な攻撃プロセスを簡単に自動化することができる。
- Villager は商業用に開発された正規のセキュリティ診断ツールを名乗りながら、攻撃にも使いやすくなっており、悪用される恐れがある。

1. Salesforce の顧客企業を狙った機密情報窃取

1.1. 概要

Salesforce の顧客を標的としたサイバー攻撃が多数、確認されている。手法として、2025 年夏には外部アプリケーションの Salesloft Drift が、またそれ以前の 2024 年秋からはソーシャルエンジニアリングが利用されている。これらにより、攻撃者は正規の操作に見せかけて Salesforce 環境への不正アクセスを実現し、大量の機密データを窃取していた。

この状況を踏まえ、2025 年 9 月には米連邦捜査局（FBI）が攻撃の高度な手口と脅迫行為についてレポートをリリースし、注意喚起を行った。

1.2. Salesloft/Drift を利用した攻撃

【Salesforce と連携する AI チャット機能「Drift」について】

Salesforce は、クラウド型の顧客管理（CRM）ソフトウェアであり、社内の各部門間で顧客情報を一元管理・共有することにより、業務効率と部門間の連携を強化する[1]。Salesforce は外部の様々なアプリケーションと連携可能であり、そのひとつが Salesloft Drift（以下、Drift）である。

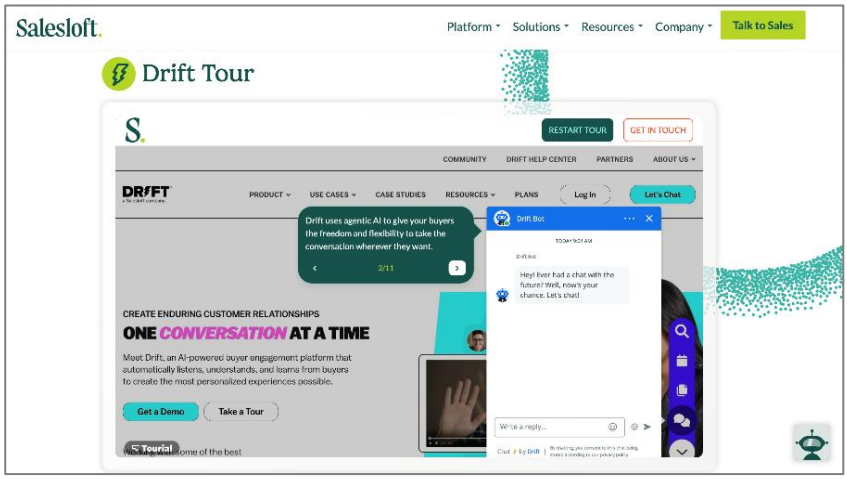

図 1 Salesloft 社の Drift 紹介ページ[2]

Drift は、営業支援プラットフォーム Salesloft に統合されている AI チャット機能である。Web サイト訪問者とリアルタイムで会話し、訪問者の属性やニーズ等を特定する機能を備えている。これにより、見込み客を営業担当者に自動的に振り分ける等、営業活動のスピードと効率を向上させることを目指している。また、会話内容を分析し、より成果につなげるよう、チャット運用の改善を支援する機能も備えている[3]。

---

[1] 出典: Salesforce『Salesforce（セールスフォース）とは？』
https://www.salesforce.com/jp/products/what-is-salesforce/

[2] 出典: Salesloft『Drift Tour』
https://www.salesloft.com/platform/drift/tour

[3] 出典: Salesloft『Drift - Convert Website Visitors Into Pipeline』
https://www.salesloft.com/platform/drift

さらに、Web サイト訪問者との会話を通じて得られた情報やチャット履歴を Salesforce に自動的に送信したり、Salesforce にある顧客情報等のデータを更新したりすることも可能となっている。これにより、リアルタイムな顧客対応とデータ管理が実現し、営業活動の効率化および成約率の向上が期待できる[4]。

【攻撃手法】

2025 年 3 月から 6 月にかけて、ある攻撃グループが GitHub （ソフトウェア開発者がソースコードを管理・共有するためのプラットフォーム）にある Salesloft 社のアカウントに、何らかの方法で不正にアクセスし、そこに格納されていたデータをダウンロードしていた[5]。

その後、グループは Drift の AWS（Amazon が提供するクラウドサービス）環境に侵入し、顧客の OAuth トークンを取得した。このトークンを利用すると、複数の Web サービスを認証済みの状態にして連動させることができる。グループはこれを利用し、8 月中旬頃、Drift と連携していた、多くの企業の Salesforce 環境にアクセスし、大量のデータを窃取した[6]。

1.3. ソーシャルエンジニアリングを用いた攻撃

【攻撃手法】

前述の事件とは別に、2024 年 10 月からは、IT サポート担当者を装った攻撃者が、Salesforce を利用する企業のカスタマーセンターの従業員に電話をかけ、相手を騙して認証情報、多要素認証（MFA）コード等を引き出すという、ソーシャルエンジニアリング攻撃が確認されている。

さらに攻撃者はターゲット企業の従業員を Salesforce のアプリケーション設定ページに誘導し、自身が用意した悪質なアプリケーション（データを一括でインポート／エクスポートできる Salesforce のアプリケーション「データローダー」の改造版）の適用を承認させるといったことも行っていた。これによりターゲット企業の Salesforce 環境から機密情報にアクセスし、それらを検索したり窃取したりすることが容易となる。このように、悪質なアプリケーションであっても Salesforce において承認されたことで、MFA やログイン監視等が回避され、長期にわたり攻撃者の不正アクセスを許す結果となった[7]。

1.4. 各社の対応

8 月 20 日、 Salesloft と Salesforce は共同で、Drift から Salesforce にアクセスするために必要だった全ての OAuth トークンを無効化する措置を講じ、攻撃経路を遮断した[8]。

---

[4] 出典: Salesloft『Drift - Integrating Drift with Salesforce』
https://help.salesloft.com/s/article/Integrating-Drift-with-Salesforce?language=en_US

[5] 出典: Salesloft Trust Portal『Update on Mandiant Drift and Salesloft Application Investigations』
https://trust.salesloft.com/?uid=Update+on+Mandiant+Drift+and+Salesloft+Application+Investigations

[6] 出典: Salesloft Trust Portal『Drift/Salesforce Security Update』
https://trust.salesloft.com/?uid=Drift%2FSalesforce+Security+Update

[7] 出典: Internet Crime Complaint Center『FBI FLASH - Cyber Criminal Groups UNC6040 and UNC6395 Compromising Salesforce Instances for Data Theft and Extortion』
https://www.ic3.gov/CSA/2025/250912.pdf

[8] 出典: Internet Crime Complaint Center『FBI FLASH - Cyber Criminal Groups UNC6040 and UNC6395 Compromising Salesforce Instances for Data Theft and Extortion』
https://www.ic3.gov/CSA/2025/250912.pdf

その後、9 月 7 日には、Salesforce と Salesloft の連携が再度、有効化されたが、Drift は当面の間、無効のままとなることが、Salesforce により発表された[9]。

なお、今回攻撃に遭った企業で、Drift を利用していた Cloudflare 社[10]や Zscaler 社[11]も攻撃による影響や対応状況について公表している。

【FBI による警告および推奨対策】[12]

9 月 12 日、米連邦捜査局（FBI）は、一連の攻撃に関して速報（レポート）をリリースした。

そしてこの中で、「（サイバー犯罪グループが）最近、異なる初期アクセス手段を用いて、Salesforce プラットフォームを標的としていることが確認されている」として、Salesforce のユーザー企業に対し、セキュリティ強化対策を提示した。具体的には、セキュリティの基本概念である「AAA（認証・認可・記録）」の導入によるユーザー操作の制限、外部連携アプリケーションの棚卸し、ならびに各アプリケーションの API キーや認証情報の定期的な更新などが挙げられている。

1.5. 犯行グループについて

8 月に明らかとなった Drift を利用した攻撃は、UNC6395（別名：GRUB1）によって実行されたとしている。一方、昨年の秋から続くソーシャルエンジニアリング攻撃には、 ShinyHunters の名で広く知られている UNC6040 の関与が疑われている[13]。両者が実際は同じ攻撃グループなのかどうかは、現時点では明確になっていない。

ShinyHunters については最近、他のハッカーグループである「Scattered Spider」および「LAPSUS$」と連携し、犯罪活動の統合を進める動きが確認されている。9 月 12 日に、Telegram 上のチャンネルにて一旦は活動終了を宣言したものの[14]、10 月初旬に「Scattered LAPSUS$ Hunters」の名でダークウェブ上にリークサイト（窃取した機密／個人情報を公開するサイト）を開設。Salesforce の顧客企業である Google 社や Cisco Systems 社を含む、計 39 社に関する、10 億件にも上るというデータの一部をサンプルとして公開した。グループは Salesforce に対して身代金の交渉を要求し、期日までに同社が応じない場合は、全ての顧客企業のデータが流出するとリークサイトで宣言していた[15]。

---

[9] 出典: Salesforce『Ongoing Security Response to Third-Party App Incident』
https://help.salesforce.com/s/articleView?id=005134951&type=1

[10] 出典: Cloudflare『Salesloft Drift の侵害が Cloudflare および当社のお客様に与える影響』
https://blog.cloudflare.com/ja-jp/response-to-salesloft-drift-incident/

[11] 出典: Zscaler『Salesloft Drift のサプライ チェーン インシデント：概要と Zscaler の対応』
https://www.zscaler.com/jp/blogs/company-news/salesloft-drift-supply-chain-incident-key-details-and-zscaler-s-response

[12] 出典: Internet Crime Complaint Center『FBI FLASH - Cyber Criminal Groups UNC6040 and UNC6395 Compromising Salesforce Instances for Data Theft and Extortion』
https://www.ic3.gov/CSA/2025/250912.pdf

[13] 出典: Internet Crime Complaint Center『FBI FLASH - Cyber Criminal Groups UNC6040 and UNC6395 Compromising Salesforce Instances for Data Theft and Extortion』
https://www.ic3.gov/CSA/2025/250912.pdf

[14] 出典: The Hacker News『FBI Warns of UNC6040 and UNC6395 Targeting Salesforce Platforms in Data Theft Attacks』
https://thehackernews.com/2025/09/fbi-warns-of-unc6040-and-unc6395.html

[15] 出典: BleepingComputer『ShinyHunters launches Salesforce data leak site to extort 39 victims』
https://www.bleepingcomputer.com/news/security/shinyhunters-starts-leaking-data-stolen-in-salesforce-attacks/

Salesforce はこのような脅迫に応じない方針を表明[16]。今回の事案については、Salesforce 本体が侵害された形跡はないと述べ、影響を受けた顧客に対しては個別対応を継続している[17]。

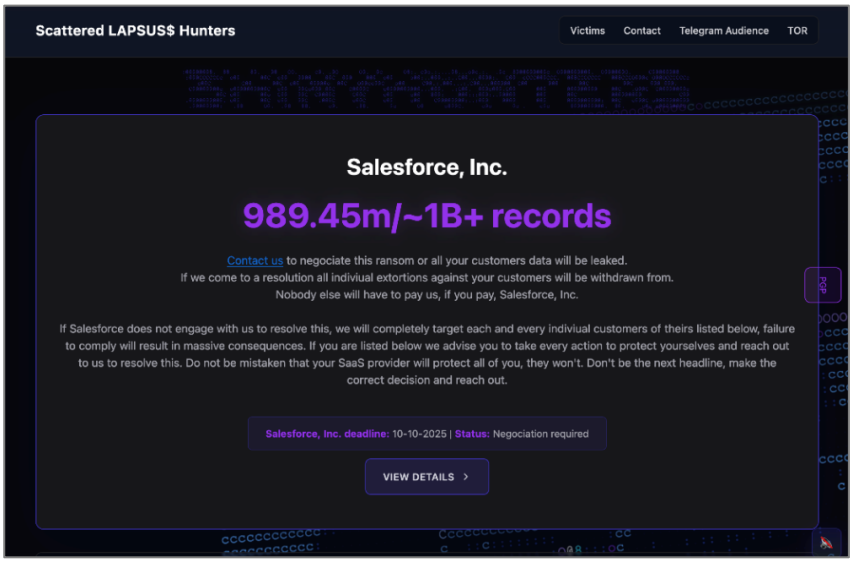

図 2「Scattered LAPSUS$ Hunters」のリークサイト

1.6. まとめ

昨年から続く一連の攻撃では、Salesforce の顧客企業の従業員を騙して認証情報を引き出す手法や、正規の外部アプリケーションである Drift の悪用が確認されており、いずれにおいても大量の重要データが多くの企業から盗まれる結果となった。Drift を介して行われたようなサプライチェーン攻撃は、効率的な手法として、引き続き多くの攻撃者の関心を集めるであろうことに留意が必要である。また、FBI の警告が示すように、企業には技術面だけでなく、人的・組織的な脆弱性にも対応した多層的な防御体制の構築が求められる。

[16] 出典: Bloomberg『Salesforce Tells Clients It Won't Pay Hackers for Extortion』
https://www.bloomberg.com/news/articles/2025-10-07/salesforce-tells-clients-it-won-t-pay-hackers-for-data-extortion

[17] 出典: Salesforce『Security Advisory: Ongoing Response to Social Engineering Threats』
https://status.salesforce.com/generalmessages/20000224

2. 新たなランサムウェア攻撃手法 ～AI による著作権侵害～

2.1. 概要

「LunaLock」という新たなランサムウェアグループが登場した。従来のランサムウェア攻撃に見られる、窃取した個人情報の公開に加えて、窃取したイラスト等のアート作品を AI モデルの学習データセットに提供するとして被害企業を脅迫する独特な手法を用いている[18]。この手法は、著作権を侵害するだけでなく、窃取されたアート作品が AI に学習されることで事実上半永久的に利用される可能性を示しており、著作権等において回復不能な侵害をもたらす点で、従来の漏洩とは異なる深刻な脅威といえる [18]。

2.2. AI モデル学習を悪用した新しい脅迫

【AI モデルと学習データ】

AI モデルに一度学習させたデータを、後から削除しようとする試みは、通常のデータベースからデータを削除することと根本的に異なる[19]。AI モデルの学習プロセスにおいてデータは、学習によって形成される膨大な数値(パラメータ)の組み合わせとして、モデル内部に複雑に組み込まれる。このため、後から特定の情報を削除することが極めて困難である [19]。改めてモデルに一から学習させない限り、過去に学習させたデータの影響を完全に削除しようとすることは現実的ではない[20]。

【LunaLock の攻撃事例】

9 月 1 日、フリーランスのアーティストとクライアントを繋ぐプラットフォームである「Artists&Clients」[21]の名が、ランサムウェアグループ LunaLock の Web サイト上に、被害企業として掲載された。このサイトで LunaLock は、「Artists&Clients」に対してランサムウェア攻撃を実行し、データベースやユーザーの個人情報、アート作品等、全てのデータを窃取し暗号化したことを主張した。さらに 5 万ドルの身代金を要求し、これが支払われない場合は当該データを公開するだけでなく、全てのアート作品を複数の AI 企業に提供して学習データセットに追加させるとも述べ、被害組織を脅迫した [18]。

---

[18] 出典: Security Affairs『LunaLock Ransomware threatens victims by feeding stolen data to AI models』 https://securityaffairs.com/182014/malware/lunalock-ransomware-threatens-victims-by-feeding-stolen-data-to-ai-models.html

[19] 出典: Digital Data Design Institute at Harvard『The Myth of Machine Unlearning: The Complexities of AI Data Removal』 https://d3.harvard.edu/the-myth-of-machine-unlearning-the-complexities-of-ai-data-removal/

[20] 出典: IBM『Why we're teaching LLMs to forget things』 https://research.ibm.com/blog/llm-unlearning

[21] 出典: Cybernews『Hackers threaten to feed data to AI if their demands aren't met』 https://cybernews.com/ai-news/lunalock-ransomware-attack-against-artists-platform/

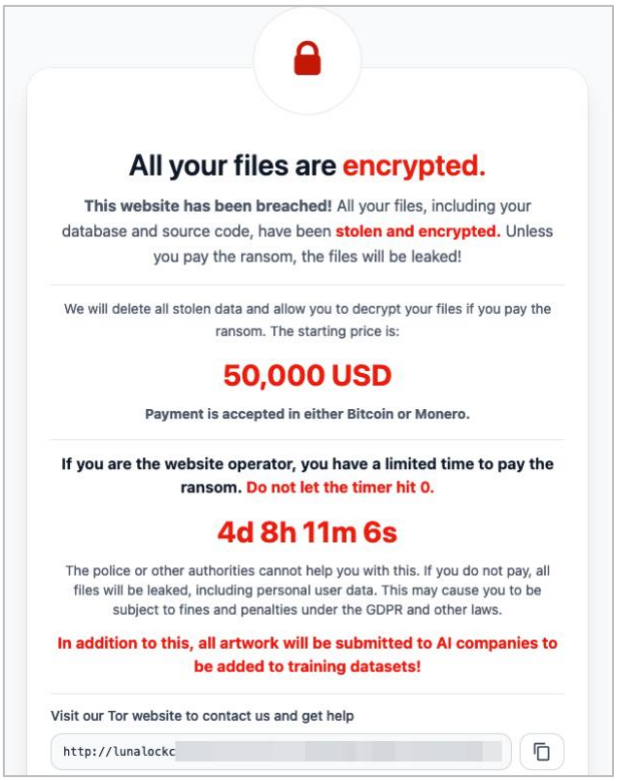

図 3 LunaLock の脅迫メッセージ[22]

【模倣の可能性と今後の懸念】

LunaLock の手法により、今後、窃取されたデータは、ダークウェブ上で公開されるだけでなく、誰でもアクセス可能な Web サイトにアップロードされ、これらのデータを収集する AI モデルによって学習に使用されるリスクが懸念される。また、今回の事は他のサイバー犯罪グループによる模倣を誘発する可能性がある[18]。

前述の通り、一度 AI モデルが学習したデータは、削除が極めて困難である。ダークウェブ上で情報漏洩が発生した場合は、最初こそ大きな影響を与えるものの、これは時間の経過とともに減少する傾向がある。一方で、AI モデルが学習したデータは半永久的に存在することになり[18]、このことは、AI を通じて著作権侵害が繰り返し発生し得る構造を生み出す可能性がある。

著作権のあるアート作品が学習データに含まれてしまうと、AI がその作品のスタイルや内容を模倣し、ユーザーの入力するプロンプト(指示や質問)に応じて、作品を再生成・再利用することが可能となる。実際に、ポーランドのアーティスト Greg Rutkowski 氏の名前は、画像生成 AI のプロンプトで約 93,000 回使用されており、彼の作風を模した画像が大量に生成されている[23]。Rutkowski 氏は、自身の名前でオンライン検索した際に AI 生成された模倣作品が多数表示されることにより、自身のオリジナル作品が検索結果の中で埋もれてしまう状況に懸念を示している[23]。

[22] 出典: X『@_venarix_』
https://x.com/_venarix_/status/1962941225335394595

[23] 出典: MIT Technology Review『This artist is dominating AI-generated art. And he's not happy about it.』
https://www.technologyreview.com/2022/09/16/1059598/this-artist-is-dominating-ai-generated-art-and-hes-not-happy-about-it/

2.3. AI による著作権侵害への社会的・技術的対応

Google の AI 関連部門や、OpenAI、Anthropic 等の主要な AI 企業がモデル学習のためにオンライン上のデータを収集している [18]。この状況について著作権の専門家は、AI モデル学習に自分の作品が許可なく使用され、その使用に対する報酬も支払われず、さらには AI ユーザーがアーティストの作品を模倣して作品を生成する行為についてもコントロールできないことを指摘している[24]。このような懸念に対し、法的・技術的な対応が始まりつつある。

【実際の裁判事例】[25]

2025 年 9 月、米国企業の Anthropic は著作権侵害をめぐる集団訴訟において、少なくとも 15 億ドルを支払うことで和解に合意した。この訴訟は、最初に 3 人の著作者が個別に訴えを起こしたことに端を発し、同様の被害を受けた著作者が加わることで集団訴訟へと発展したものである。原告側は、同社が海賊版共有サイトから入手した書籍を使用して、チャットボット「Claude（クロード）」を訓練したことが著作権侵害にあたると主張していた。和解の対象となる書籍数は推定 50 万点であり、Anthropic は 1 作品あたり約 3,000 ドルを著作者に支払うことと、ダウンロードした書籍ファイルを破棄することに同意した。裁判所によりこの和解が承認されれば、著作権関連の賠償金としては史上最大となる。

【アート作品を保護するツールの登場】

シカゴ大学の Ben Zhao 教授によって開発された Glaze や Nightshade 等、画像生成 AI の無断学習に対抗するためのツールが、作品を保護する手段として注目されている [18]。

Glaze は、画像に微細な加工を施すことで、AI モデルがこの画像を本来の作品とは異なるスタイルとして誤認するよう誘導する防御的なツールである[26]。一方、Nightshade は画像を、AI モデルに誤学習させるような構造に変換する。これにより、アーティストに無断でその作品を AI モデルに学習させたとしても、これを使用する AI は予測不可能で不正確な画像を生成する。このツールは AI モデルの学習精度を低下させ、画像の模倣に対する抑止となっている [26]。

これらのツールが、2022 年のリリース以来 300 万回以上のダウンロードを記録していることからも、インターネット上でアート作品を公開する多くのアーティストらが、AI による作品の無断学習に対して懸念を持っていることが伺える [18]。

2.4. まとめ

被害者のアート作品を無断で AI モデルの学習材料にすると脅す LunaLock の手法は、従来のデータ漏洩とは異なり、被害者の著作権等を半永久的に侵害する。今回の事件は、デジタル化が進む現代において、人間の独創性が生かされるべき分野が直面する新たな脅威を浮き彫りにしており、AI 企業側での対策が急がれる。

---

[24] 出典: Los Angeles Times『As AI is embraced, what happens to the artists whose work was stolen to build it?』 https://www.latimes.com/opinion/story/2024-06-18/artificial-intelligence-openai-media-manager-apple

[25] 出典: NPR『Anthropic to pay authors $1.5B to settle lawsuit over pirated chatbot training material』 https://www.npr.org/2025/09/05/g-s1-87367/anthropic-authors-settlement-pirated-chatbot-training-material

[26] 出典: Ars Technica『Tool preventing AI mimicry cracked; artists wonder what's next』 https://arstechnica.com/tech-policy/2024/07/glaze-a-tool-protecting-artists-from-ai-bypassed-by-attack-as-demand-spikes/

3. 中国発 AI ペネトレーションテストツール「Villager」

3.1. 概要

AI を活用したペネトレーションテストツール「Villager」(ヴィレジャー)のダウンロード数が、リリースから 2 か月後の 9 月時点で 1 万回を超えた。このツールは、中国拠点のグループ「Cyberspike」が開発している。Villager を利用すれば、専門知識がなくても高度な攻撃プロセスを簡単に自動化することができる。本来は企業の防御力を高める目的でセキュリティ診断時に用いるツールだが、誰でも容易に扱えるため悪用されるリスクも高いことが懸念されている[27]。

3.2. Villager について

【これまでのペネトレーションテストツール】

ペネトレーションテストツールとは、セキュリティの専門家が運用中のシステム全体に対して、あえて攻撃を仕掛けることでセキュリティ対策の有効性を評価するために用いる模擬ハッキングツールである。

以前は、このようなツールを使用してハッキングを実行するためには、ハッカーの視点からどのようにターゲットのシステムに侵入するかを考えながら、複雑な攻撃プロセスを作成する必要があった。これには専門知識を持つ人間の判断力や想像力が不可欠なことから、攻撃プロセスを自動的に作成することは難しいとされてきた。

【専門知識がなくても高度な攻撃が構築できる Villager の登場】[28]

Villager(Villager Pentesting Tool) は、中国の Cyberspike によって、Python で開発されたソフトウェアを共有できるサイト PyPI(Python Package Index)にて 7 月下旬から公開されており、誰でもダウンロードができる。

このツールにおいては、セキュリティ専門家向けに特化された OS である Kali Linux のセキュリティツール群(ポートスキャン用の Nmap やパケットキャプチャ用の Wireshark 等が含まれる[29])と DeepSeek AI モデルが統合されていることにより、AI が状況を判断し、攻撃テストのための最適な手法を作成する。人が曖昧な目標を Villager に与えると、AI が必要な情報を集めて偵察・脆弱性診断・侵入・ネットワーク内での潜伏までを自動化する。そのための指示も日常的に使う自然な言語で行うことが可能である。

例えば、「example.com の脆弱性を見つけて悪用する」というタスクを Villager に送信すると、同ツールはドメインや公開されているポートの番号といった、ターゲットのシステム環境に関する情報を調査し、検出結果に基づいて攻撃手法を調整する。攻撃は段階ごとに達成を確認しながら進められ、侵害に成功すると永続的な監視が行われる。活動ログは 24 時間で削除され、証拠隠滅が図られる。

---

[27] 出典：Straiker『Cyberspike Villager – Cobalt Strike's AI-native Successor』
https://www.straiker.ai/blog/cyberspike-villager-cobalt-strike-ai-native-successor

[28] 出典：Straiker『Cyberspike Villager – Cobalt Strike's AI-native Successor』
https://www.straiker.ai/blog/cyberspike-villager-cobalt-strike-ai-native-successor

[29] 出典：OffSec Services Limited『Kali Tools』
https://www.kali.org/tools/

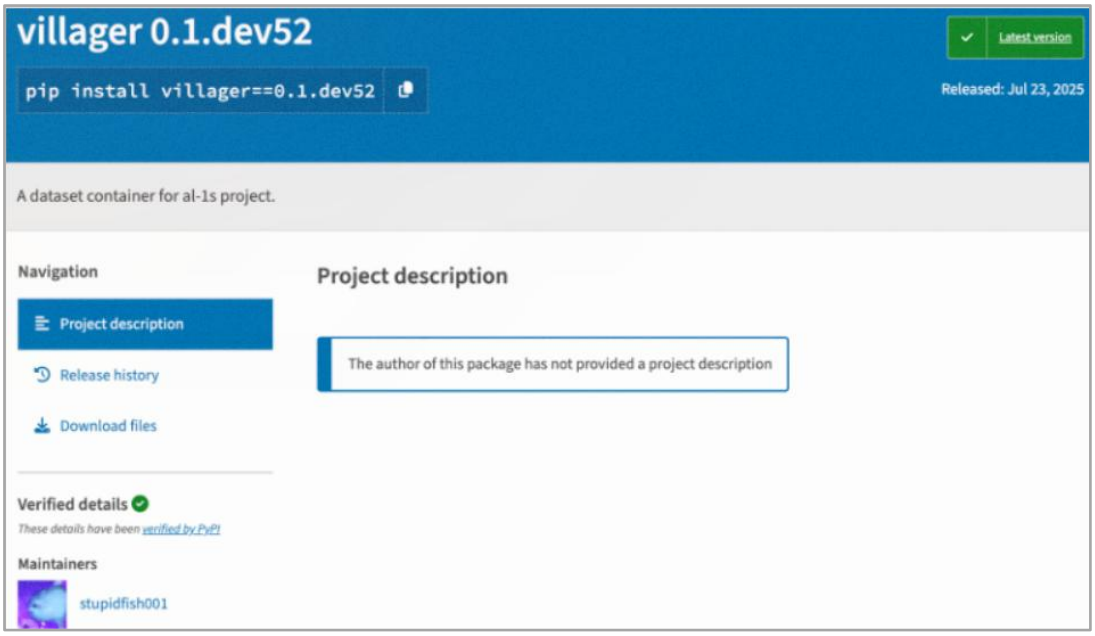

図 4 PyPI の Villager のサイト[30]

【Cobalt Strike の AI 後継】[31]

正規のセキュリティツールの悪用というと、マルウェアキャンペーンや国家支援型攻撃グループがよく利用していた「Cobalt Strike」が知られている。このツールは商用の攻撃シミュレーションツールで、組織が自身のネットワークの防御力を確認するためにセキュリティテストを行うことができるよう、開発された。ただし操作には高度な専門知識が必要だった。

操作性と効率を飛躍的に高めた Villager は、サイバー攻撃における Cobalt Strike のポジションに収まる可能性が考えられることから、「Cobalt Strike の AI 後継」ともいわれている。

3.3. Cyberspike グループについて

Cyberspike は、AI を活用したサイバーセキュリティツールを開発している中国のグループである。しかし、このグループの実態について明らかにされていることは少ない。

組織と同名の cyberspike.top というドメイン名の使用は、リポジトリのアカウントやソースコードの中に見られる。WHOIS 情報を参照すると、このドメイン名が 2023 年 11 月に、中国の企業「長春安山源科技有限公司(Changchun Anshanyuan Technology Co., Ltd.)」によって初めて登録されたことが確認できる[32]。

[30] 出典：Straiker『Cyberspike Villager – Cobalt Strike's AI-native Successor』
https://www.straiker.ai/blog/cyberspike-villager-cobalt-strike-ai-native-successor

[31] 出典：Straiker『Cyberspike Villager – Cobalt Strike's AI-native Successor』
https://www.straiker.ai/blog/cyberspike-villager-cobalt-strike-ai-native-successor

[32] 出典：Straiker『Cyberspike Villager – Cobalt Strike's AI-native Successor』
https://www.straiker.ai/blog/cyberspike-villager-cobalt-strike-ai-native-successor

図 5 cyberspike.top ドメインの登録情報[33]

この企業は、レッドチーム(攻撃者側の視点でセキュリティテストを行うためのチーム)が使用するツールおよび AI 関連ツールの開発に従事しているとされているが、これが正当な事業であることを示す証跡は確認できない。また Cyberspike の所属の実態や背景も明らかになっていない。ただ、数少ない情報の一つとしては、過去に Cyberspike が開発したツールが、リモートアクセス用の既知のマルウェアと組み合わせて販売されていたことが挙げられる[34]。

3.4. まとめ

Villager は AI を使って自然な言語で誰でも簡単に侵入テストが自動化できるという、技術的にもよくできた先進的なツールである。商業用に開発された正規のセキュリティ診断ツールを名乗りながら、実際は攻撃にも使い易くなっており、悪用される恐れがある。スキルの低いハッカーでも、このようなツールを使うと、これまで高度な攻撃と考えられたものを容易に実現してしまうことが考えられる。今後のセキュリティ環境が大きく変わる可能性があり、本ツールや同様なツールの発展状況については注意が必要である。

以上

[33] 出典：兴宁市漫游科技有限公司『ICP 备案查询』
https://icplishi.com/cyberspike.top/

[34] 出典：Straiker『Cyberspike Villager – Cobalt Strike's AI-native Successor』
https://www.straiker.ai/blog/cyberspike-villager-cobalt-strike-ai-native-successor

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