MITRE | The MITRE Center for Technology & National Security

本ニュースは、弊社パートナーillusive networksに転写されたMITRE社のホワイトペーパーを翻訳し、注釈を付加したうえで掲載しています。原文は注釈をご覧ください

サイバースペースの優位性：罠への誘導

サイバーDeceptionが可能にする強靭化の方法

By Deborah L. Schuh

サイバースペースの優位性：罠への誘導

サイバーDeceptionが可能にする強靭化の方法

サイバー強靭化："サイバーリソースを使用する、または使用可能なシステムに対する不利な条件、ストレス、攻撃、または侵害を予測し、抵抗し、回復し、適応する能力。"
- 米国国立標準技術研究所（NIST）による
特別刊行物800-160第2巻（案）

サイバー脅威に強いシステムを構築するためには、敵が予測できず、回避できず、攻撃できないような技術や手法を採用することが必要です。

一つの方法は、システムに特殊な目的のハードウェア、オペレーティング・システム、ソフトウェアを組み込むことで、そのシステムにしかない「特別なソース」を作り、敵に知られないようにすることです。
また、システムの耐障害性を高めるには、NISTの文書に記載されている非永続性や多様性などの技術を採用することもあります。これらのメカニズムは、敵対者が我々の最も重要な資産に足場を築く能力を制限することができますが、サイバーセキュリティには、短期的にも長期的にも利益をもたらす、見過ごされがちなアプローチがあります。

サイバー防御に欺瞞を取り入れることで、悪意のある行動を検知したり、侵入した敵を管理したり、敵の戦術や技術に関する情報を収集したりすることができます。欺瞞から得られるサイバーインテリジェンスは、防御と回復力をより引き出すことができます。

ボーイング社の787型機のコード流出が教えてくれる非対称な優位性の創出について

2019年7月7日、『WIRED』は、サイバー研究者が無防備なボーイング社のネットワークサーバーを発見したことをめぐる論争を報じました。2018年9月、サイバーセキュリティ研究者のRuben Santamartaは、インターネットで旅客機の情報を調べていたところ、787乗務員情報サービス／メンテナンスシステムのソフトウェアが置かれているボーイングのサーバーを偶然発見しました。Santamartaは、保護されていないサーバーがハッカーにアクセス可能であること、ソフトウェアに重大なセキュリティ上の欠陥があることを公にしました。

この記事を読んだほとんどの読者は、ボーイング社の787型旅客機の品質と安全性、そしてサイバー事故の可能性に関心を持ったかもしれません。しかし、もしこの研究者が、ボーイング社が監視している中で、高度なサイバー攻撃者が収集することを目的とした、現在では無効となっている古い設計情報の意図的な公開に遭遇していたとしたらどうでしょうか。今回の話がそうでないとしても、全体的なサイバー戦略の一環として真剣に検討すべきことだと思います。

今から何年も前、MITRE コーポレーションは、自社のネットワーク内に高度なサイバー脅威（APT：Advanced Persistent Threatとも呼ばれる）を発見したときに、ある難問に直面しました。

MITRE社はこれを機に、敵の手法や戦術について詳しく知ることにしました。スタッフが、環境内を移動するAPTの行動や技術を監視し、データを収集する環境を作りました。その結果、攻撃者に関する貴重な情報を得ることができ、防衛目的で他の組織と共有することができました。しかし、MITRE社では、これまでサイバーインシデントや侵入の報告がなかったため、MITRE 社が攻撃者の行動に関する情報をどのようにして得たのか疑問視する声もありました。このようにして、私たちはサイバーDeceptionの領域に足を踏み入れたのです。[1]

サイバーDeceptionは何が新しいのでしょうか?

サイバーDeceptionの基本（ハニーポット、ハニーネット、ハニートークンなど）は数年前から存在していますが、敵の手法や行動パターンをより深く理解しようとする組織の動きに合わせて、真のDeceptionの技術も高まっています。欺瞞のためのツールや専門知識を提供するマーケットが出現し、急速に成長しています。

現在の技術では、既存のインフラの中にDeception環境を迅速に構築し、既存のサイバー防御システム（侵入検知システムなど）に接続することができます。例えば、組織は、意図的に敵をおびき寄せるための高度なDeception環境を構築することができます。偽のユーザーや認証情報、侵入者を活動的にさせるのに十分な価値のある偽の情報や誤解を招くような情報、侵入者をナビゲートするためのネットワーク情報などを、観察可能な制御された環境の中で提供することができます。サイバーDeceptionの製品や専門知識は、これまで以上に入手しやすく、また手頃な価格になっています。

Deceptionの基本

ハニーポット、ハニーネット、ハニートークン、ポケットリッターは、潜在的なサイバー攻撃者にとって安全性が低く魅力的になるように特別に作られたコンピュータリソースや情報資産を指す言葉です。ハニーポット、ハニーネット、ハニートーク、ポケットリッターは、安全性が低く、潜在的なサイバー攻撃者にとって魅力的なコンピュータリソースや情報資産の総称です。これは、社内のシステムやネットワークにパラレルワールドを作り、敵の注意をそらして、敵を封じ込めたり観察したりすることができる管理された環境に誘導するというものです。

ハニーポットとは、ウェブサーバやファイルサーバなどのホストコンピュータで、攻撃者がホストを操作したり、データを盗んだり、漏洩させたり、ターゲットネットワークをさらに調査したりするように仕向けるものです。

ハニーネットは、複数のハニーポットで構成されたネットワークです。ハニーポットとハニーネットは、実際のネットワークをエミュレートするように構成されており、攻撃者は実際のネットワーク環境への侵入に成功したと錯覚します。

ハニートークンとは、通常のユーザーには見えない偽のデータ（文書、URLなど）や認証情報のことで、これにアクセスすると悪意のある活動を示すことになります。通常、警告メカニズムとして使用されます。

ポケットリッターとは、ハニーネット上のユーザーを、関連する文書、アカウント、Webブラウザの履歴などでシミュレートし、欺瞞環境に現実感を与えるための情報です。ポケットリッターがリアルであればあるほど、攻撃者は自分が実際のネットワークにいると錯覚する可能性が高くなります。

[1] For more information, read Cyber Denial, Deception and Counter Deception: A Framework for Supporting Active Cyber Defense, Kristin E. Heckman et al., Springer International Publishing, 2015.

“すべての戦争は欺瞞に基づいている

攻撃できるときはできないように、兵力を使うときは活動してないように、近くにいるときは敵に遠くにいると思わせ、遠くにいるときは近くにいると思わせなければなりません。” 孫子

サイバーDeceptionの意味

国防科学委員会や政府説明責任局が多くの報告書で明らかにしているように、国防総省（DoD）は、兵器や企業システムにおけるサイバーセキュリティとレジリエンスの導入にいまだに苦慮しています。従来のセキュリティ対策ではもはや十分ではないことが明らかになりつつあります。Deceptionは、攻撃者に対して重要な知識と優位性を得る機会を提供することで、たくさんのメリットがあります。

1. 敵対者の発見と管理。現在市販されているDeceptionツールは、悪意のある行動を警告する自動化機能を備えていますが、誤認識はほとんどありません。敵対者を封じ込めたり、意図的なターゲットに誘い込んだりすることができます。

2. 敵の技術を学ぶことで、より良い防衛情報を得ることができます。攻撃者の手法やテクニックを観察して捕らえることは、より優れたサイバー防御やレジリエンスを構築する上で非常に重要です。また、敵のアイデンティティを明らかにできるような方法で環境を感知することで、欺瞞性を向上させることができます。

3. 内部脅威の発見。外部の敵を検知するために使用されるDeception技術は、内部の悪意ある脅威の検知も可能にします。Deception環境は、パターンではなく存在に基づいているため、あらゆる形態の疑わしい行動に警告を発するように構成されています。

4. より良いインシデント対応。アラートと監視を組み合わせることで、環境で何が起こっているのかをより明確に捉え、理解することができます。これにより、より効率的で効果的な対応が可能になります。

5. 攻撃者を欺くこと。ネットワーク、ポケット・リター、ハニートークンを巧みに利用することで、攻撃者の時間とリソースを浪費させ、その血統を明らかにし、攻撃者側に誤った知識を植え付けることができます。また、Deceptionによって、アーキテクチャ、ネットワーク・トラフィック、サービス、ミッション・アクティビティにランダム性や予測不可能性が加わり、攻撃者が環境を理解することが困難になり、最悪の場合、不正確になります。

軍事的な領域では、高度なDeception環境は、より高度な軍事目的を達成するために非常に慎重な方法で使用することができます。

知識の共有による投資収益率の向上

Deceptionと観察によって得られた知識は、国防総省内の同種のシステム間で迅速に共有されるべきです。すべてを意図的に機密化して共有しないという対改竄性の道を歩むことは、サイバー脅威に対処する際には有用ではなく、賢明でもありません。サイバー脅威の現れ方はさまざまで、瞬時に変化し、悪意に満ち、蔓延しています。敵の戦術、技術、手順（TTPs）に関する貴重な情報を隠しておくと、国防総省は不利な立場に立たされます。サイバー環境は非常に頻繁に変化しており、脅威は非常に広範囲に及んでいるため、攻撃者の作戦をタイムリーに共有することが、脅威を把握し、企業全体でより良い防御を可能にする唯一の方法なのです。

[2] Anti-tamper technology applies mechanisms that prevent or slow unauthorized reverse engineering of sensitive electronic equipment, computers, software, and other technologies critical to creating U.S. military advantage.

サイバー脅威情報の特性評価と共有を可能にする規格やフレームワークが存在します（CAPEC™[3]、STIX™[4]、TAXII™[5]、ATT&CK™[6]、NTCTF[7]）。これらの規格は、主に情報技術を利用したサイバー攻撃に対応するために策定されたものですが、兵器や組み込みシステム（サイバーフィジカルシステムとも呼ばれる）における敵のTTPの特徴を把握するために拡張されています。これらの拡張により、脅威の理解、情報の共有、そしてこれらのユニークなタイプの資産の防御が可能になります。

最も重要な資産を守るために

国防総省は、サイバーDeceptionから得られる脅威の情報を他のサイバーインテリジェンスと組み合わせて、重要な資産のより良い防衛に役立てるべきです。

最低限、国防総省全体で戦略的にDeceptionを展開すべきであり、特に敵の関心や意図が分かっているシステムにはDeceptionを導入すべきです。Deceptionの機能をフルに活用し、得られた知識を活用して、防衛やDeception自体を継続的に改善していくべきです。

これと並行して、国防総省は複数のミッションや企業にとって最も重要な資産を強化する必要があります。それは、多くの作戦システムやミッションの基盤となる共通のコンポーネントや機能を提供する資産です。位置決め、ナビゲーション、タイミング、通信、内部バス、ラジオ、プログラマブル・ロジック・コントローラ、エンジン、その他の重要な機能を提供するコンポーネントは、すべて硬化の恩恵を受けます。

すべての主要な兵器システムを堅牢化させることはコスト的に不可能ですが、共有されている重要なコンポーネントを堅牢化させることは可能です。

コンポーネントの堅牢化には、ベンダーと直接協力して、これらのデバイスに組み込まれている耐障害性の高い技術を開発するための投資が必要です。
また、攻撃者がアクセスできないような特殊な目的のハードウェアやソフトウェアを独自に開発することも必要です。このような投資は、既存の記録的なプログラムに結びつけることはできませんが、効果的かつ効率的に行うためには、企業レベルでの管理と資金調達が必要です。

国防総省は、攻撃者がアクセス可能な商用オフザシェルフ（COTS）コンポーネントに大きく依存していることに疑問を持つべきです。国防のサイバーセキュリティミッションの重要性は、COTSソリューションを評価する際の方程式の一部でなければなりません。COTSコンポーネントは、兵器システムよりも、一般的なインフラ、ビジネスシステム、「一般的なコンピューティング（関連するサイバーセキュリティやDeception製品も含む）」に適しています。

商用市場は、国防総省がすべきことほど、進行中の洗練されたサイバー「戦争」に強く動かされていません。それは、第二次世界大戦のように、一般の人々にとって目に見える紛争ではありません。しかし、防衛産業基盤（DIB）にとっては、この対立は目に見えるものであり、堅牢で弾力性のあるコンポーネントを開発するための効果的なパートナーでなければなりません。また、DIBは、APTによる知的財産や軍事データの持続的な流出に何年も直面しており、Deceptionを展開する上で効果的なパートナーとなることができます。

[3] Common Attack Pattern Enumeration and Classification (CAPEC™) provides a comprehensive dictionary of known patterns of attack employed by adversaries to exploit known weaknesses in cyber-enabled capabilities.
[4] Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence. STIX enables organizations to share threat information with one another in a consistent and machine-readable manner.
[5] Trusted Automated Exchange of Intelligence Information (TAXII™) is an application-layer protocol for communicating cyber threat information as represented in STIX. Visit https://oasis-open.github.io/cti-documentation/ for more on STIX and TAXII.
[6] MITRE ATT&CK™ is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. https://attack.mitre.org/
[7] NSA/CSS Technical Cyber Threat Framework (NTCTF) is a National Security Agency standard for characterizing adversary activity with a common technical lexicon closely aligned with industry definitions. This common technical cyber lexicon supports sharing, product development, operational planning, and knowledge-driven operations across the Intelligence Community.

成功とは何か?

国防総省とDIBは、継続的に防御力を向上させ、サイバーレジリエンスを高める必要があります。これを成功させるには、新しいアイデア、新しい戦略、そして新しいパートナーシップが必要です。

1. 国防総省は、国防総省のシステムとDIBに戦略的にDeceptionを展開すべきです。これをうまく行うことで、攻撃者に関する貴重な知識を集め、攻撃者の封じ込めと管理によるより良い防衛を可能にします。

2. 様々なDeception環境から得られた情報を同種のシステムのコミュニティと共有することで、敵のテクニックと効果的な防御策の両方に関する総合的な理解を深めることができます。

3. システムにCOTSを採用する度合いを再評価し、調整する必要があります。この方程式の一部として、すでに流出したデータの量や、APT が利用できるその他の情報を調べる必要があります。これにより、サイバーセキュリティとレジリエンスのために必要な保護を決定することができます。

4. 国防総省の企業全体で重要な共通コンポーネントを堅牢化させることは、多くのシステムのハードルを上げることになり、コンポーネントのベンダーと直接協力して行わなければなりません。

サイバー防衛のパワーバランスを変えることは難しく、敵についての知識を深め、サイバー脅威の情報を効果的に共有し、国家安全保障に最も重要な資産の保護と回復力を向上させることが、成功につながります。

著者について

Deborah Schuhは、MITRE コーポレーションのサイバー戦略・チーフセキュリティオフィスのサイバー統合担当ディレクターです。サイバー、システム工学、運用の専門知識を駆使して、国防省が抱えるサイバー分野の難題に取り組んでいます。

MITRE Center for Technology & National Securityに関して

MITRE社は、Center for Technology and National Security (CTNS)を設立し、今日の競争の激しい戦略的環境で成功するために必要なデータに基づいた分析と技術的な情報に基づいた洞察を国家安全保障のリーダーに提供しています。このセンターは、米国の利益を高め、国家安全保障を強化するために、政策立案者がダイナミックで急速に進化するテクノロジーの状況をよりよく把握できるよう支援することを目的としています。CTNSは、非営利・超党派のMITRE Corporationの一員として、米国で最も尊敬されている数千人の科学者や技術者の経験と専門知識に基づいて構築されています。同センターは、政府、学界、産業界、メディア、政策研究機関から専門家や有力者を集め、前例のない技術変化の時代に情報に基づいた議論を推進しています。

MITRE社の使命感あふれるチームは、より安全な世界のために問題解決に取り組んでいます。連邦政府から資金提供を受けている研究開発センターや官民パートナーシップを通じて、政府全体で国家の安全性、安定性、福利に対する課題に取り組んでいます。

【訳者付加注釈】

◆ 本ホワイトペーパーの出典

- illusive networks
  https://go.illusive.com/mitre-white-paper-deception-endorsement-for-cyber-resilience
- MITRE
  https://www.mitre.org/publications/technical-papers/the-cyberspace-advantage-inviting-them-in

◆ 単語集

- NIST
  米国国立標準技術研究所(National Institute of Standards and Technology)の略称

- サイバーインテリジェンス
  情報通信技術を用いた情報収集・諜報活動。外交や安全保障に重大な影響が生じる可能性がある情報収集。

- レジリエンス
  攻撃を受けたとき、その影響を最小化し、早急に元の状態に戻す仕組みや能力のこと。

- 対改竄性（アンチタンパー）
  攻撃者が改竄・改変することを困難にすること

- TTPs
  Tactics, Techniques, and Proceduresの略

- COTS
  Commercial Off-The-Shelfの略

- DIB
  the Defense Industrial Baseの略

MITRE

MITRE Center for Technology and National Security