2024 年 10 月 16 日

< Topics >

サイバー攻撃の活動を隠蔽する新たな手法に警鐘

日本電信電話株式会社（以下、「NTT」）と NTT セキュリティホールディングス株式会社（以下、「NTT セキュリティ」）は、サイバー攻撃においてマルウェアの悪意ある動作を隠蔽する新たな手法を発見し、現実的な脅威として実現可能であることを明らかにしました。サイバー攻撃が巧妙化し検知が難しくなっているなかで、このような新しい脅威を攻撃者に先んじて発見することは、セキュリティ上重要な取り組みと言えます。本成果は、2024 年 8 月 7 日から 2024 年 8 月 8 日に開催された Black Hat USA 2024 Briefings にて発表されました(*1)。Black Hat USA 2024 Briefings の採択率は約 8 %となっており、サイバーセキュリティ分野において最難関の産業系国際会議として知られています。非常に狭き門である本会議への採択は、サイバーセキュリティ分野の世界トップレベルの成果として認められたことを意味します。今後は、攻撃の手口に関する情報をセキュリティ製品等の開発者と共有し本脅威に備えるとともに、NTT グループのセキュリティサービスや攻撃者視点でのセキュリティ検証を目的とするレッドチーム活動等を通じて、新たな脅威に対する早期発見・対応に取り組んでいきます。

■ Bytecode Jiu-Jitsu: Choking Interpreters to Force Execution of Malicious Bytecode
雉井 利宣 研究主任（NTT セキュリティ）、大月 勇人 主任研究員（NTT セキュリティ）

【研究成果】

サイバー攻撃で利用されるマルウェアの悪意ある動作を隠蔽する技術のひとつにコードインジェクションがあります。従来のコードインジェクションは、良性プロセスのメモリ空間に実行権限付きのメモリ領域を確保し、悪性コードを書き込み、その悪性コードを実行する、という特徴的な手続きが必要であり、セキュリティ製品による検知の手がかりとなっていました。

NTT および NTT セキュリティは、本研究において実行権限付きのメモリ領域の確保や

明示的なコード実行を必要とせずに、良性プロセスへの悪性コードの書き込みのみで実現可能な新たなコードインジェクション手法を発見しました。プログラムの実行方法のひとつとして、ソースコードをいったん中間コードに変換して実行する仕組みがありますが、新手法ではその中間コードを悪性のものに書き換えることで、良性プロセスに紛れ込ませて実行させることを可能にします（図 1）。

実験では、本手法が既存のセキュリティ製品による検知を回避可能なことを確認しました。この結果を踏まえ、セキュリティ製品等の開発者に対して攻撃手法に関する情報を共有するとともに、本脅威への備えについて連携を進めています。

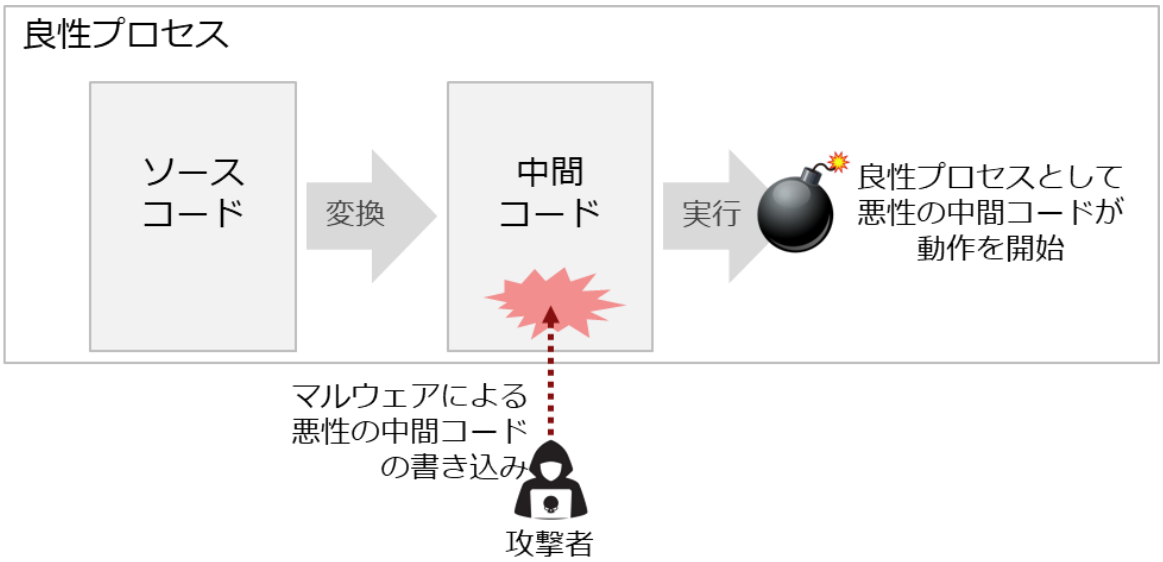

図 1 新たなコードインジェクション手法

(*1) Toshinori Usui, Yuto Otsuki, Ryo Kubota, Yuhei Kawakoya, Makoto Iwamura, Kanta Matsuura, ”Bytecode Jiu-Jitsu: Choking Interpreters to Force Execution of Malicious Bytecode”, https://blackhat.com/us-24/briefings/schedule/#bytecode-jiu-jitsu-choking-interpreters-to-force-execution-of-malicious-bytecode-38682.

【お問い合わせ先】
NTT セキュリティホールディングス株式会社
makoto.iwamura@security.ntt