2012 年 9 月 11 日
(2012 年 10 月 23 日更新)
独立行政法人情報処理推進機構(IPA)

ICS-CERT/US-CERT Joint Security Awareness Report
JSRA-12-241-01B-Shamoon/W32.DistTrack マルウェア

本概要は、米国土安全保障省の運営する ICS-CERT(Industrial Control Systems Cyber Emergency Response Team)と US-CERT(United States Computer Emergency Readiness Team)が発行する、"JSAR-12-241-01B-Shamoon/DistTrack Malware)"の抄訳となります。内容の詳細につきましては、原文をご参照ください。(※本文中のリンク先は全て英文となります)
URL: http://www.us-cert.gov/control_systems/pdf/JSAR-12-241-01B.pdf

概要

W32.DistTrack、通称"Shamoon"は、システム破壊モジュールを持つ情報窃取型マルウェアである。感染すると、マスターブートレコード(MBR)、パーティションテーブル、ファイルなどをランダムなデータで書換え、コンピュータを使用不能にする(書換えられたデータは復旧不能)。
現状、Shamoon が制御システムや米国政府機関を標的にしていると断じる証拠は見つかっていない。

シマンテック社によれば、Shamoon は 3 つのモジュールから構成されている。

1. Dropper:核となるモジュール。最初にコンピュータを感染させ、他のモジュールをインストールする
2. Wiper:破壊機能を担うモジュール
3. Reporter:攻撃者への情報送信を担うモジュール

感染後は、ネットワークを通じて他のコンピュータに感染を広げる。シマンテック社が最初に Shamoon を発見したのは 2012 年 8 月 16 日であるが、その時点での感染は殆どなかったと推察されている(世界で 50 台以下)。

影響

Wiper モジュールの高いシステム破壊機能により、感染した組織は知的財産(IP)の窃盗、重要システムの停止など、運用上の影響を受ける可能性がある。感染したシステムの種類や数によって、実際の影響度は異なる。

対策

ICS-CERT では、以下の対策の実施を奨励している。実際に対策を行う前に、影響分析とリスク評価を行うこと。

＜戦術的対策＞

＊＊＊＊＊ 更新 B ここから ＊＊＊＊＊

- 復旧計画の実施訓練を行う

- 内部ネットワーク上に、以下のような、Shamoon の亜種のリクエストと一致する通信がないか監視・検知する
  http://<internal_C&C_IP>/ajax_modal/modal/data.asp?mydata=<_iteration>&uid=<IP>&state=<random number>
- システム上に ElRawDisk ドライバが存在しないか、確認する

＊＊＊＊＊ 更新 B ＊＊＊＊＊

- 重要なファイルは、ネットワーク上で共有し、バックアップを可能にする
- 全ての重要システムについて、日次バックアップを実施する
- 重要ファイルを、リムーバブルメディアなどのオフライン媒体に定期的にバックアップする
- ネットワークリソースが使用できなくなった場合のため、緊急通信手段を確保しておく
- 重要なネットワーク（制御システム運用ネットワークを含む）は全て、業務ネットワークから分離する
- 重要システムを特定し、有事にサービスを迅速に復旧するために、予備品を確保しておく必要性の有無を検討する
- ウイルス対策ソフトは常に最新の状態に更新しておく。亜種は検知できないという報告もあるが、それでも、ウイルス定義ファイルの更新は必須となる
- サーバなど、重要システムにとって特に機器の認証情報はキャッシュしない（無効化する）。また、ポータブル機器の認証情報のキャッシュも出来る限り制限する。この実現には、グループ・ポリシー・オブジェクト（GPO）の利用が考えられる
- リムーバブルデバイスの自動実行（AutoRun）機能と自動再生（AutoPlay）機能を無効化する
- 業務遂行上の必要性がある場合を除き、マルウェアの拡散や侵入、およびデータの取り出しを制限するため、リムーバブルメディアの使用を防止、または制限する。業務遂行上の必要性については、メディアがどのように使用されるべきかを定めたポリシーやガイダンスに基づき、組織の最高 IT 責任者（Chief IT Security Officer）の承認を得なければならない
- アカウント権限の制限を検討する。特定の機能の実行に管理者権限が必要でない場合に限り、通常業務については標準のユーザアカウントで実行することを奨励する。全ての標準ユーザアカウントでは、未知のソフトウェアや未承認のソフトウェアのインストールは実行できないように設定する。また、「職務権限の分離」の概念を実現し、標準アカウントも管理者権限アカウントも、通常業務の遂行に最低限必要なサービスにのみアクセスできるものとする。最後に、管理者権限アカウントのウェブおよび電子メールの使用を無効化する。管理者権限アカウントの乗っ取りは、ネットワーク環境における非常に執拗な攻撃活動を可能にしている一因となっている
- Admin アカウントに対するパスワードポリシーの適用、および Admin アカウント用パスワードの定期的な変更を確実に行う
- 本番環境または DMZ 内のホストが、他のネットワーク上のホストと Active Directory を共有するのを禁止する。各環境は、Active Directory 内にそれぞれ別のフォレストを構成し、可能であればフォレスト間における一切の信頼関係の成立を許可しないようにする。必要であれば、低信頼性環境から高信頼性環境に対する一方向の信頼関係とするべきである
- クリックによって受諾するページの提供を検討する。この方法は従来より、ネットワークの利用規定

の受諾記録や、利用状況をモニタリングすることをユーザに通知するのに使われている。また、こうしたページは、自動化された悪意ある攻撃活動を防ぐ対策も提供する。これは、自動化された攻撃では、通常ラジオボタンを物理的にクリックすることができないことによる。自動化された攻撃は実行するようハードコード化されており、その後、インターネットからコマンドや他の実行ファイルを取って来る。マルウェアがインターネットへの接続を確立できない場合、フルスケールの感染は阻止される。ユーザが物理的に許可してしまう危険性は引き続きあるが、こうしたページを置くことにより、感染を制限できるか、少なくとも感染速度を遅らせることができる

- ログの監視　－　異常な活動や、潜在的に攻撃と考えられる活動を追跡する、中央集約的なログを運用・監視する
- 全てのネットワーク OS、ウェブブラウザ、その他、関連するネットワーク機器やソフトウェアについて最新のパッチや修正の適用を確実に行う

＜戦略的対策＞

- パッチは常に最新のものが適用されているようにする。ファイアウォールを通して公共サービス（HTTP、FTP、電子メール、DNS サービスなど）を提供するコンピュータについては特に注意する
- ホストシステムの構築、とりわけ、サーバなど重要システムの構築は、意図する機能の実行に必須なアプリケーションおよびコンポーネントのみ入れる。可能であれば、ホストシステムへの攻撃の間口を狭めるため、使わないアプリケーションや機能は、取り除くか、無効化する
- マルウェアの拡散を制限するため、VLAN を使ってネットワークをセグメント化する
- 許可されたアプリケーションしか実行できないように設定したソフトウェア制限ポリシー（Software Restriction Policy）の適用を検討する（ソフトウェア・ホワイトリスティング）
- 潜在的に攻撃と考えられるバイナリファイルの実行を防ぐため、正当な実行ファイルの一覧を使ったホワイトリストティングが奨励される
- 特権を有するルートレベルアカウントやシステムへのアクセスについては、二因子認証を奨励する
- セキュアなリモートアクセスのため、スプリット・トンネリングを禁じた IPSec/VPN ゲートウェイを用いて、二因子認証の実装・展開を検討する
- プロキシを経由したエンタープライズサーバやワークステーションを除き、インターネットへの直接アクセスは行わない。プロキシやファイアウォールでは、定期的なコンテンツ・フィルタリングを実施する。また、明示的 vs.透過的なプロキシーポリシーの実装・展開を検討する
- 潜在的に攻撃と考えられる活動のインバウンド／アウトバウンドの暗号化通信を検査するため、セキュア・ソケット・レイヤ（SSL）検査機能を実装する
- セキュアでマルチテナントな可視化技術を活用し、電子メール、ウェブアプリケーションサーバなどのネットワークサービスを分離する。これによって、1 つのネットワークコンポーネントに対する攻撃と侵害による損失が制限される
- 基幹データやシステムへのアクセスや処理に、基幹システムに属さない情報資産を使用することを制限するため、ベストプラクティスガイダンスおよびポリシーを実践する（例：家からのリモートアクセス、オフィスにおける個人所有機器の使用など）。企業の資産でない機器に対する企業ポリシー適用の徹底、侵入の検知、フォレンジック分析の実施、問題の是正は難しい
- 業務遂行上の必要性がある場合を除き、オフィスにおける私的な電子メール、インスタントメッセー

ジ、フェイスブック、ツイッターなどのソーシャルネットワーキングサービスの利用を制限する。業務遂行上の必要性は、組織の最高IT責任者（Chief IT Security Officer）の承認を得なければならない。正当な業務上の必要性がある場合は、データの紛失やマルウェアの脅威といったリスクを低減するガイダンスおよびポリシーを実践する

- 制御システム機器のネットワークへの接続を最低限に絞り込む。制御システム機器は、直接インターネットに接続しない
- 制御システムネットワークをファイアウォールで守る。また、企業の業務ネットワークから隔離する、または水も漏らさぬようにセキュリティを固める
- リモートからのアクセスが必要な場合、VPNなどセキュアな手段を用いる。但し、VPNのセキュリティの強度は、接続機器のセキュリティの高さ（弱さ）に準じることを理解したうえで検討する

サイバーインシデントに遭った場合の検知と復旧に関しては、ICS-CERT Technical Information Paper ICS-TIP-12-146-01A Cyber Intrusion Mitigation Strategies（サイバー侵害緩和対策）も参照可能。

また、「制御システムセキュリティプログラム（CSSP：Control System Security Program）」でも、US-CERTウェブサイト上で、他にも推奨するセキュリティ対策を纏めたドキュメント等も提供しており、Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies（多層防御戦略による産業制御システムのサイバーセキュリティ改善）などが参照可能。

以上