2019 年 7 月 23 日

サービス＆セキュリティ株式会社 e-Gate センター

リモートデスクトップサービスの脆弱性「BlueKeep」について

1. はじめに

リモートデスクトップサービス（RDS）とは、Windows にリモートでログオンし、データへのアクセスやアプリケーションの実行などの遠隔操作ができるサービスです。

2019 年 5 月の月例セキュリティ情報において、Microsoft は RDS における脆弱性（CVE-2019-0708）を修正する更新プログラムを公開しました。この脆弱性は「BlueKeep」と名付けられ、2017 年に甚大な被害をもたらしたランサムウェア「Wanna Cryptor」に匹敵する被害をもたらす危険性が指摘されています。Microsoft がすでにサポート終了している「Windows XP」などの OS に対しての更新プログラムを公開する異例の対応をとったことも、その危険性を物語っています。

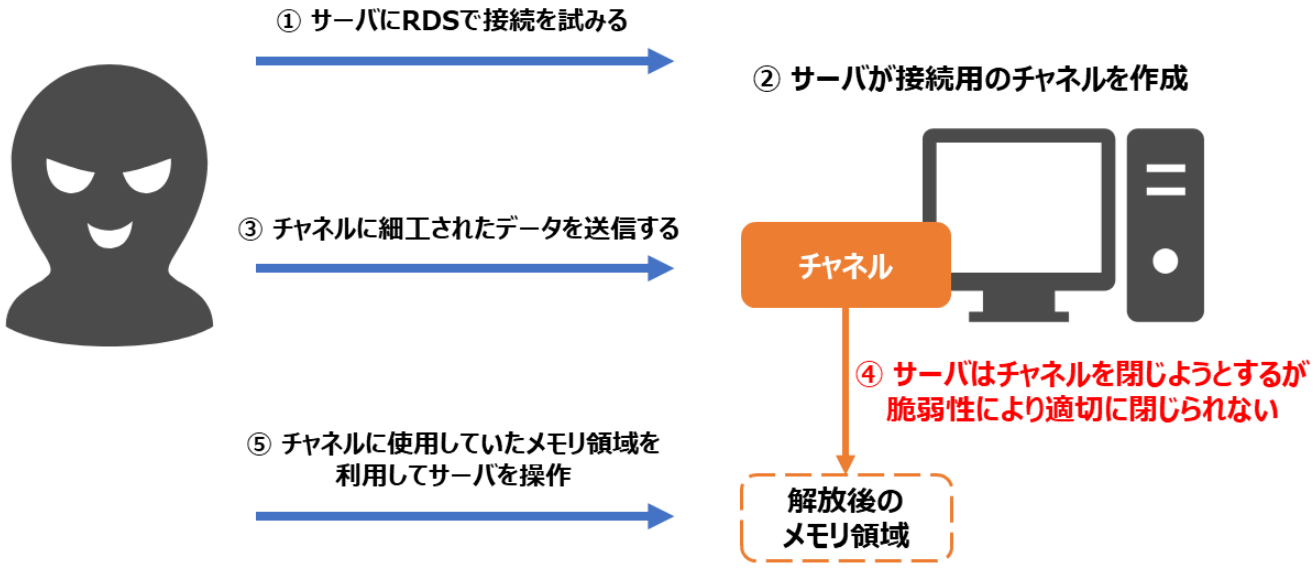
そこで本記事では、「BlueKeep」の特徴と対策をご紹介いたします。

2. BlueKeep の攻撃について

2.1 攻撃の流れ

RDS において、クライアントは遠隔サーバの TCP ポート 3389（デフォルト設定）に対してリモートデスクトッププロトコル(RDP) で通信を行います。

この通信において、以下のような手順でサーバを乗っ取ることができます。

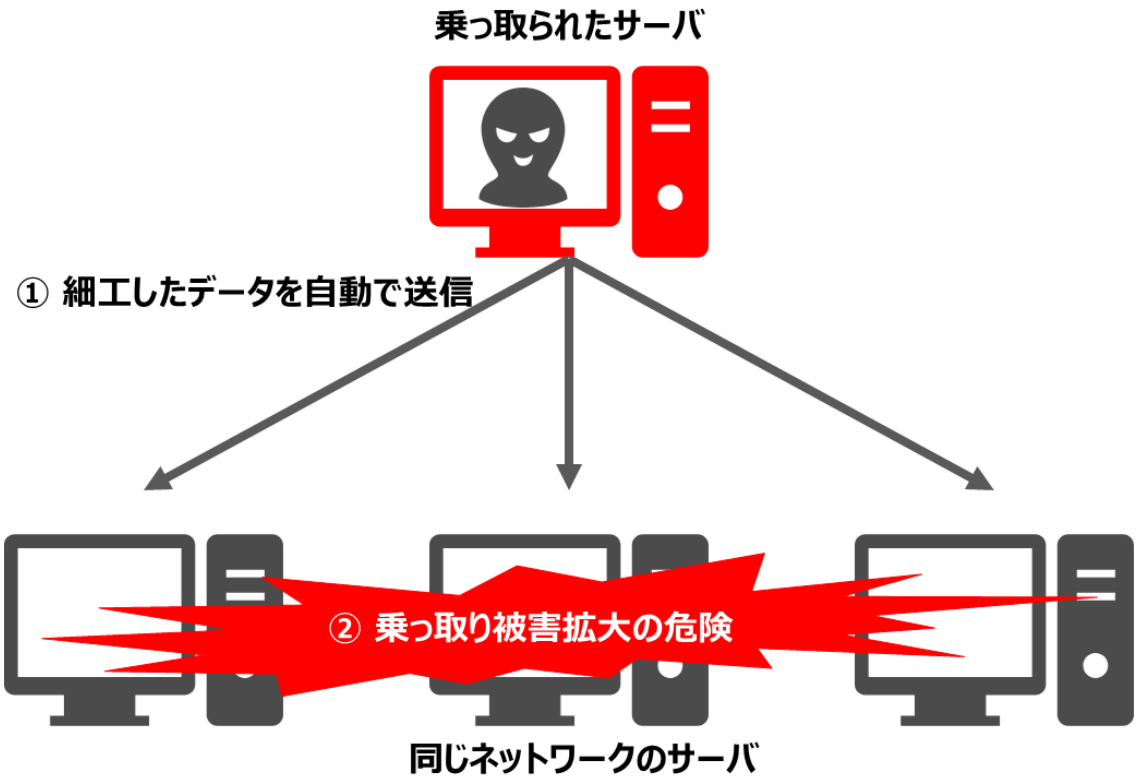


【図 1：攻撃の流れ】

③の細工されたデータの送信は RDS のユーザー認証の前に行われるため、アカウント名やパスワードを知らなくてもサーバを乗っ取ることができます。接続に成功した場合、攻撃者が管理者権限を手に入れてしまい、悪意のあるプログラムをインストールしたり、すべての権限を持つ新しいアカウントを作成したりすることが可能になり、気づかないうちにサーバを乗っ取られてしまいます。

2.2 特徴

- ワームのような特性



【図 2：被害拡大のイメージ】

攻撃対象となったサーバからさらに別の端末に細工したデータを送信することで、ワームのように自動的な拡散が可能です。1 つの端末が攻撃を受けてしまうと、ネットワーク内の他の端末も攻撃の対象となってしまう可能性があります。

- 古い Windows が対象

この脆弱性の対象として発表されたのは以下のバージョンであり、サポートが終了したものが含まれています。

- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003
- Windows 7
- Windows Vista
- Windows XP

古いバージョンであるとはいえ、それらのバージョンのシステムがいまだに利用されているケースも少なくありません。前述のよう

に Microsoft がそれらのシステムに対する更新プログラムを配布していることも、これが重大な問題であることを裏付けているといえるでしょう。

3. 対策

- 最新のアップデートを適用する

  脆弱性を修正する更新プログラムを Microsoft が公開しています。対象バージョンのシステムを使用している場合、インストールすることが推奨されます。

- RDS を無効にする

  この脆弱性は RDS を利用したものであるため、必要ない端末の RDS を無効にしておくことも有効な対策であるといえます。その上で更新プログラムをインストールするとさらに確実です。

- TCP ポート 3389 に向けた通信をブロックする

  RDP はデフォルト設定で 3389 ポートを使って通信を行うため、当該ポートへの通信を Firewall や IPS（侵入防御システム）などで遮断することも一定の効果が見込めます。SecureSoft Sniper IPS では 2019 年 6 月に配信されたシグネチャ ID 4791 によって当該脆弱性に対応しています。ただし、Firewall や IPS で遮断できるのは外部からの侵入であるため、内部のネットワークから侵入される場合には効果がないことにご注意ください。

4. e-Gate の監視サービスについて

Firewall や IPS をはじめとするセキュリティ機器を導入する場合、それらの機器の運用監視を行うことが重要です。“e-Gate”の 24 時間 365 日有人監視体制のセキュリティ監視サービスをご活用頂きますと、最新の分析システムを活用し精度の高い検知、専任のアナリストによる分析、迅速なセキュリティインシデント対応支援でセキュリティ対策を強化することが可能です。“e-Gate”の MSS の導入をぜひご検討ください。

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた IT 運用のノウハウと、最新のメソッド、次世代 SOC“e-Gate センター”この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”です。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】

https://www.ssk-kan.co.jp/e-gate/

5. 参考情報

- Microsoft
  CVE-2019-0708 のユーザー向けガイダンス
  https://support.microsoft.com/ja-jp/help/4500705/customer-guidance-for-cve-2019-0708
  CVE-2019-0708 | リモート デスクトップ サービスのリモートでコードが実行される脆弱性
  https://portal.msrc.microsoft.com/ja-jp/security-guidance/advisory/CVE-2019-0708
- IPA（情報処理推進機構）
  Microsoft 製品の脆弱性対策について(2019 年 5 月)
  https://www.ipa.go.jp/security/ciadr/vul/20190515-ms.html
- JPCERT
  リモートデスクトップサービスにおける脆弱性 CVE-2019-0708 について
  https://www.jpcert.or.jp/newsflash/2019051501.html

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。
リンク先のコンテンツは予告なく、変更、削除される場合があります。

«お問合せ先»
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp