レポート

令和元年6月 21 日

リモートデスクトップサービスを標的としたアクセスの増加等について

- リモートデスクトップサービスを標的としたアクセスの増加について
- Oracle WebLogic Server の脆弱性(CVE-2019-2725)を標的とした探索活動等の観測

1 リモートデスクトップサービスを標的としたアクセスの増加について

警察庁のインターネット定点観測において、平成 31 年 3 月下旬頃からリモートデスクトップサービスを標的とした広範囲の宛先ポートに対するアクセスの増加を観測しました(図1)。

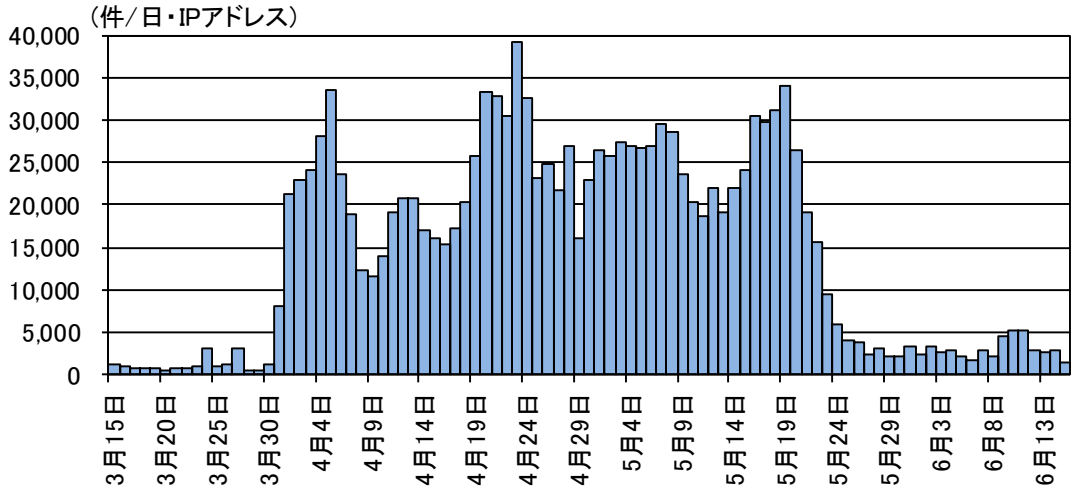

図1 リモートデスクトップサービスを標的としたアクセス件数の推移(H31.3.15～R1.6.15)

同アクセスにおいて、リモートデスクトップサービスのサーバに接続する際に送信される、特定の文字列を含むパケットを観測しています(図2)。

図2 観測したアクセスの例(一部抜粋、マスキングを実施)

リモートデスクトップサービスは、Microsoft Windows の遠隔操作に使用されるサービスで、主にポート 3389/TCP を使用しますが、今回観測したアクセスでは、ポート 3389/TCP を含む広範囲の宛先ポートに対するアクセスを観測しています(図3)。

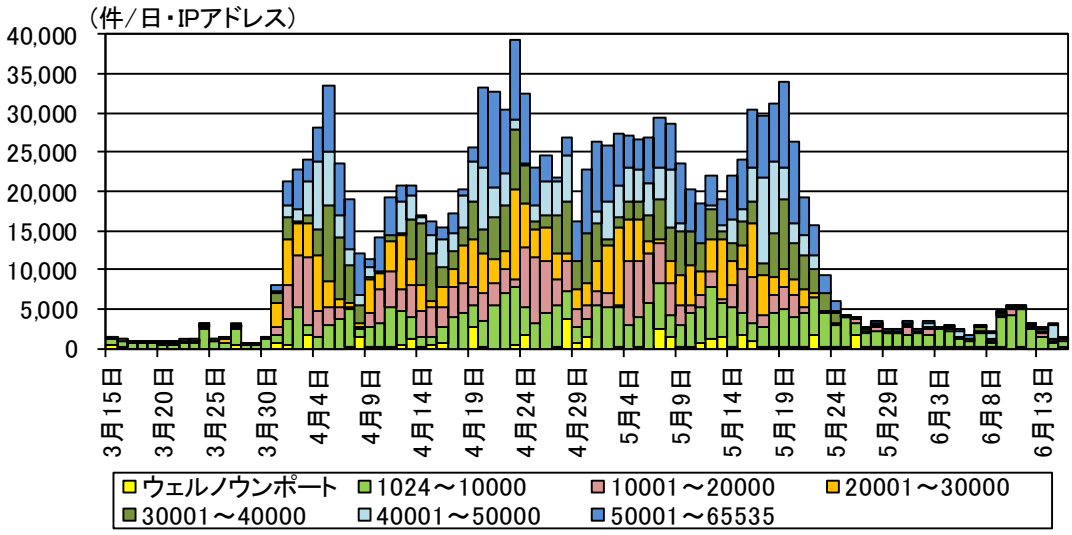

図3　リモートデスクトップサービスを標的とした広範囲の宛先ポート(TCP)に対するポート別アクセス件数の推移（H31.3.15～R1.6.15）

同アクセス内容に着目すると、広範囲の宛先ポートに対して特定の IP アドレス帯からのアクセスを多数観測していることから、3389/TCP 及びそれ以外のポートで稼働するリモートデスクトップサービスの探索行為が行われていると考えられます。

また、マイクロソフト社は 5 月 15 日にリモートデスクトップサービスの脆弱性（CVE-2019-0708）を修正するプログラムを公開しました。既にサポートが終了している Windows XP や Windows Server 2003 向けの修正プログラムを提供[i]するなど、異例の対応がなされています[ii]。

リモートデスクトップサービスの脆弱性（CVE-2019-0708）は通称「BlueKeep」と呼ばれており、攻撃対象のシステムに細工した接続要求を送信することで、任意のコードを実行することが可能とされています。当該脆弱性が公表された後、既に特定の条件でブルースクリーンを発生させる検証コード（PoC[iii]）が存在していることを確認しています。また、当該脆弱性の存在を確認するためのリモートスキャンツールがインターネット上に公開されています。

リモートデスクトップサービスの利用者は、以下の対策を参考にセキュリティ対策を行うことを推奨します。

- マイクロソフト社が公開する修正プログラムを適用し、OS を最新の状態にしてください。
- リモートデスクトップサービスを使用しない場合、当該サービスを無効にしてください。

---

[i] 「CVE-2019-0708 のユーザー向けガイダンス | 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: 2019 年 5 月 15 日」
https://support.microsoft.com/ja-jp/help/4500705/customer-guidance-for-cve-2019-0708

[ii] 「Prevent a worm by updating Remote Desktop Services (CVE-2019-0708)」
https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/

[iii] Proof of Concept の略

- リモートデスクトップサービスを用いてインターネット経由で接続する場合には、特定の IP アドレスのみにアクセスを許可するなどの適切なアクセス制限を実施してください。
- リモートからアクセス可能なユーザを必要最小限に限定してください。
- ユーザ名及びパスワードは推測されにくいものにしてください。
- 3389/TCP 以外のポートを用いてリモートデスクトップサービスを運用している場合であっても、上記の対策を講じることを強く推奨します。

2 Oracle WebLogic Server の脆弱性（CVE-2019-2725）を標的とした探索活動等の観測

Oracle WebLogic Server は Oracle 社が開発販売するソフトウェア製品であり、Java EE でウェブアプリケーションを作成する際に利用されるアプリケーションサーバです。平成 31 年4月 26 日に Oracle 社から Oracle WebLogic Server に存在する脆弱性（CVE-2019-2725）[i] が公表されました。同社は、当該脆弱性が悪用された場合、未認証でネットワーク経由による攻撃が可能としています。

警察庁においては、国外の複数のウェブサイトに当該脆弱性の有無を確認するためのものとされるソースコードや当該脆弱性を悪用することができるとされるソースコードが公開されていることを確認しています。また、4月 25 日以降、当該脆弱性の有無を確認する探索行為や悪用を試みていると思料されるアクセスを観測しました（図4）。

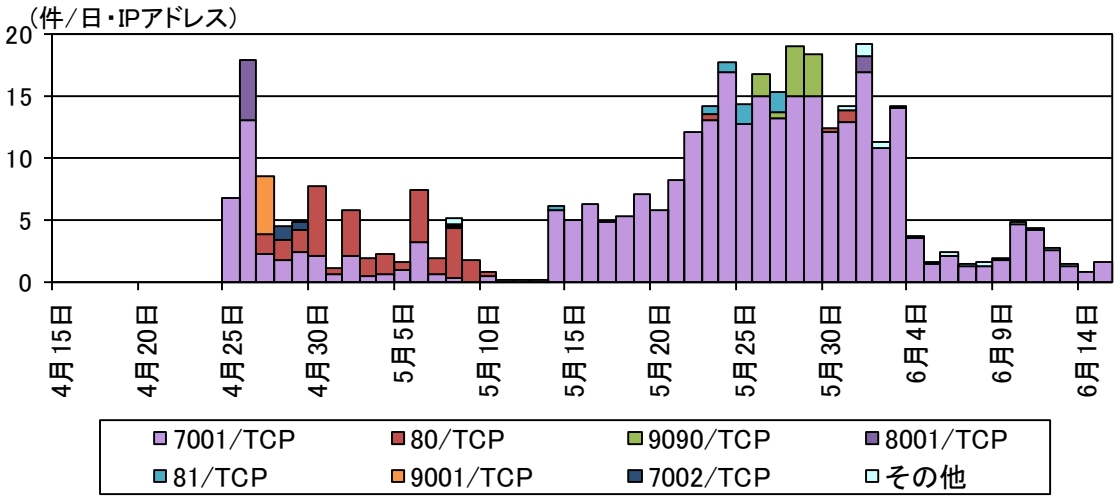

図4 Oracle WebLogic Server の脆弱性（CVE-2019-2725）の探索行為や攻撃活動と思料されるアクセス件数の推移（H31.4.15～R1.6.15）

Oracle WebLogic Server を利用している場合には、以下の対策を実施することを推奨します。

- Oracle 社から当該脆弱性の修正プログラムが入手できる場合は、アップデートの実施を検討してください。
- Oracle WebLogic Server の管理用に利用するポート（7001/TCP 等）や一般の利用者がアクセスする必要がないポートについては、インターネットからのアクセスを遮断する又は特定の IP アドレスからのみアクセスを許可するなどの適切なアクセス制限を実施してください。
- アップデートされないまま管理用ポートがインターネットからアクセス可能となっていた Oracle WebLogic Server は、既に攻撃を受けている可能性があります。該当するサーバ等に不審なプロセス、ファイル、通信等が存在しないか確認してください。

[i] 「Oracle Security Alert Advisory – CVE-2019-2725」
https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html