2020 年 05 月 15 日

サービス＆セキュリティ株式会社 e-Gate センター

e-Gate にて観測：DrayTek 社製ルータ Vigor の脆弱性（CVE-2020-8515）を利用した攻撃の増加

1 概要

DrayTek 社製ルータ「Vigor」の脆弱性（CVE-2020-8515）を利用した攻撃が世界的に急増しており、e-Gate センターにおいても多数観測しています。本脆弱性を未修正のまま使用している場合、早急なアップデートが必要です。また、本脆弱性の放置により、すでに攻撃を受けていないかご確認ください。

本記事では、DrayTek 製ルータ「Vigor」の脆弱性とその脆弱性を利用した攻撃により拡大するボットネットを取り上げ、そこから一般的な脆弱性対策についてご紹介いたします。典型的な事例のため、本機器を使用していない場合でもご参考にしていただき、今後に備えてください。

2 DrayTek 社製ルータ「Vigor」の脆弱性

DrayTek 社製ルータ「Vigor」の脆弱性（CVE-2020-8515）が 1 月 31 日、NVD にて公開[1]されました。本脆弱性の対象となるバージョンは以下の表のようになります。

【表 1】CVE-2020-8515 の脆弱性対象一覧

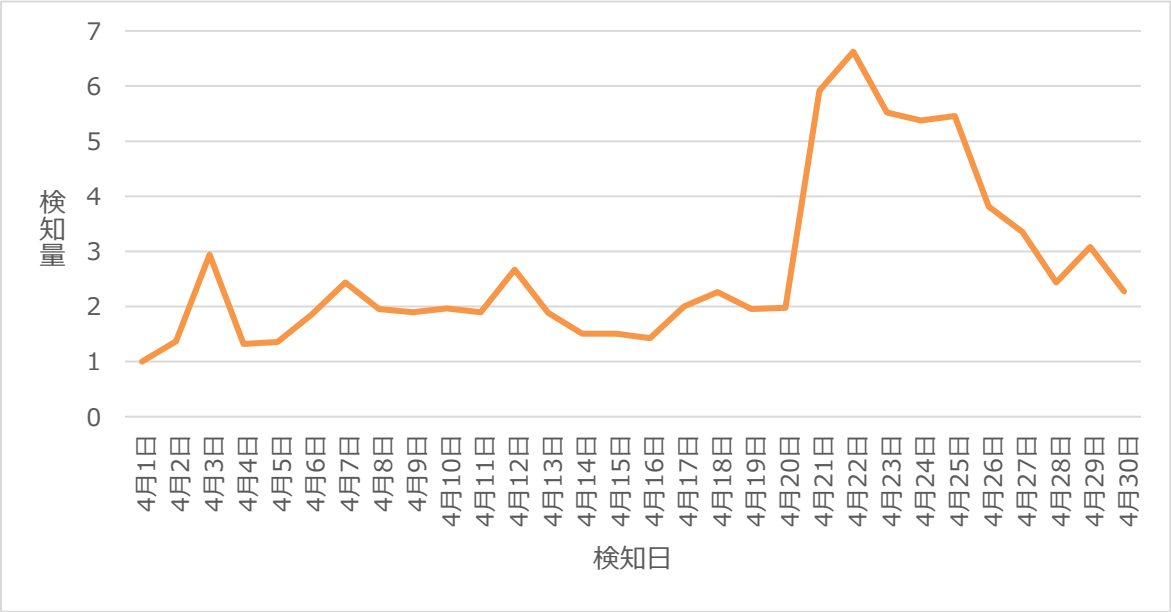
脆弱性対象機器名	脆弱性対象ファームウェアバージョン
Vigor300B	1.3.3_Beta 1.4.2.1_Beta 1.4.4_Beta
Vigor2960	1.3.1_Beta
Vigor3900	1.4.4_Beta

攻撃者によって本脆弱性を突かれると、リモートでルート権限を取得され任意のコマンドを実行されます。「任意のコマンドを実行される」とは文字通り攻撃者が望む好きなコマンドを実行することが可能ということであり、たとえば機器の内部にマルウェアを仕掛けたり、機器の情報を盗むことができたりします。この脆弱性は特別な攻撃条件を必要としないため、脆弱性の深刻度を表す値 CVSSv3 は 9.8（最大値 10.0）と非常に高くなっています。

2 月 10 日、同社は本脆弱性を修正したバージョンのファームウェアを公開[2]しました。利用ユーザはこの更新を行うことで脆弱性を解消することができます。しかし、情報がいきわたっていないユーザや、更新を躊躇しているユーザがいることを考慮すると、脆弱性を残したままインターネットにつながっている本機器が存在していることが想定されます。

そのような中、3 月 31 日に PoC（実証コード）と呼ばれる本脆弱性に対する具体的な攻撃コードが公開されたことにより、世界中でこの攻撃コードを含む通信が急増しました。修正版のファームウェア公開から 1 か月以上経過後、攻撃通信が増加した形となっています。

この攻撃は弊社 e-Gate センターにおいても多数観測しています。図 1 に、4 月中の e-Gate センターでの検知推移を示します。21 日～25 日にかけての大幅な増加は収束していますが、依然として高い検知量を維持しています。今後しばらくは高水準の検知量が継続すると予想されます。



【図 1】e-Gate センターにおける CVE-2020-8515 に対する攻撃通信の検知推移
※検知量は、4 月 1 日の件数を 1 としたときの割合を示します。

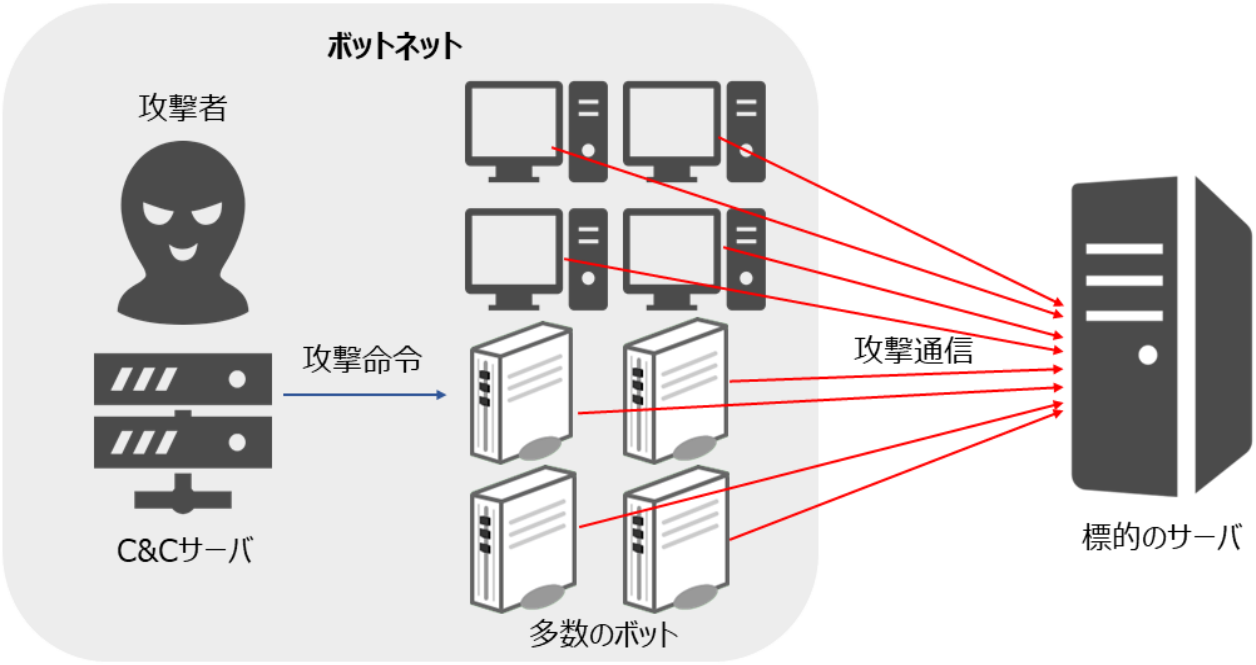
3　脆弱性を突かれることによるボット化およびボットネットの形成

機器の脆弱性を突かれた場合、様々な影響が考えられます。脆弱性がある機器に含まれる情報を窃取されるだけにとどまる場合もあれば、そこを足掛かりに内部ネットワークに侵入し、別の機密情報を窃取、改ざんされる場合もあります。Palo Alto Networks 社の調査[3]によれば、本脆弱性を利用し、機器を「ボット」化させる動きが見受けられるようです。

脆弱性を突かれ、攻撃者に乗っ取られた機器は「ボット」と呼ばれます。ボットは攻撃者の C&C（Command and Control）サーバにより操られた状態であり、任意のコマンドの実行を命じられるとそのコマンドを実行させられてしまいます。攻撃者が侵入した機器にて、C&C サーバと通信できるプログラムを仕掛けるなどされることによりその機器はボット化し、攻撃者の意のままに操られます。

さらに攻撃者はボットを増やし、多数のボットと C&C サーバからなる「ボットネット」を形成します。1 つのボットからの通信は微量ですが、それが多数集まることで一度に多量の通信を行うことができます。たとえば、標的のサーバに対して一斉に通信を行うことにより標的のサーバの負荷を増大させ、サービスを停止させる攻撃（DDoS 攻撃）など、影響が甚大となるサイバー攻撃を行うことが可能です。図 2 にボットネットによる攻撃の概念図を示します。

ボットネットに組み込まれた場合は、はじめは被害者であった機器の利用ユーザが加害者となり得る点に、特に注意が必要です。送信元の IP アドレスは真の攻撃者のものではなく、機器自体の IP アドレスが使われます。攻撃を受けた被害者が攻撃通信の送信元 IP アドレスを調査した結果、機器の所有者が判明し、損害賠償を請求される可能性もあります。



【図 2】ボットネットによる攻撃の概念図

4　対策

2 章では機器の脆弱性に対する攻撃、3 章ではボット化した機器からの攻撃をご紹介しました。本章では、これらの攻撃を防ぐためにどのような対策をすべきかについて述べます。なお、ここで紹介する対策は本脆弱性に限ったものではありません。一般的な脆弱性対策としてご参照ください。

① 自社で使用している機器やソフトウェアのバージョンを把握し、脆弱性情報を日々収集、更新する

使用している製品の脆弱性情報が公開されたときには、ソフトウェアのアップデートによって早期に脆弱性を解消することが脆弱性に対する基本的な対処方法となります。そのためには自社で使用している機器やソフトウェアのバージョンを把握し、脆弱性情報を日々収集、更新することが必要です。

脆弱性情報の収集はツールによって効率化できる場合があります。対応 OS が限られますが、IPA では「Vuls」という OSS の脆弱性管理システムの例が紹介[4]されています。

② FW、IPS などのネットワークセキュリティ機器を導入する

本記事で紹介したルータのように、脆弱性を気にすべきネットワークにつながる製品は多岐にわたります。そのため、使用している機器すべてにおいて脆弱性を持たない状態を保ち続けることは困難です。また、稼働中のシステムについて更新による影響を検討した結果、更新を見送る判断をする場合もあります。

そこで、FW、IPS などのネットワークセキュリティ機器を導入することが次の対策となります。ネットワークセキュリティ機器は脆弱性を突く攻撃を検知し、設定次第では遮断させることができます。これにより、更新が追い付かず脆弱性を抱えたまま稼働している機器への攻撃を未然に防ぐことができます。

なお、①が不完全な場合だけに限らず、完璧にできていたとしてもこうした機器を導入することをお勧めします。な

ぜなら、脆弱性を突く攻撃だけではなく、DDoS 攻撃やパスワードを総当たりで試すブルートフォースアタックなどといった、機器の脆弱性によらない攻撃の対策をすることも可能だからです。

③ ネットワークセキュリティ機器を適切に運用する

ネットワークセキュリティ機器導入後は、それらの機器の適切な運用が不可欠です。サイバー攻撃は 24 時間 365 日いつでも行われる可能性があることからリアルタイム監視が欠かせません。さらに、ネットワークセキュリティ機器が出力するログを分析し、危険性を判断する必要があります。

しかし、社内だけでこれらの運用を行うには多くのコストがかかってしまいます。そこで、外部の SOC（セキュリティオペレーションセンター）にネットワーク機器の運用をアウトソーシングするという手段がございます。

5 章にて、弊社 SOC の”e-Gate センター”についてご紹介しております。ぜひご覧ください。

5 e-Gate の監視サービスについて

e-Gate のセキュリティ機器運用監視サービスでは、24 時間 365 日、リアルタイムでセキュリティログの有人監視を行っております。サイバー攻撃への対策として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い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。e-Gate のセキュリティ監視サービスをご活用いただきますと、迅速なセキュリティインシデント対応が可能となります。

また、e-Gate の脆弱性診断サービスでは、お客様のシステムにて潜在する脆弱性を診断し、検出されたリスクへの対策をご提案させていただいております。

監視サービスや脆弱性診断サービスをご活用いただきますと、セキュリティインシデントの発生を予防、また発生時にも迅速な対処が可能なため、対策コストや被害を抑えることができます。

■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」と最新のメソッドで構築した「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”サービスです。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/

6 参考文献

[1] NVD - CVE-2020-8515 （2020 年 5 月 13 日 参照）
https://nvd.nist.gov/vuln/detail/CVE-2020-8515

[2] Vigor3900 / Vigor2960 / Vigor300B Router Web Management Page Vulnerability (CVE-2020-8515) | DrayTek （2020 年 5 月 13 日 参照）
https://www.draytek.com/about/security-advisory/vigor3900-/-vigor2960-/-vigor300b-router-web-management-page-vulnerability-(cve-2020-8515)/

[3] Grandstream and DrayTek Devices Exploited to Power New Hoaxcalls DDoS Botnet （2020 年 5 月 13 日 参照）

https://unit42.paloaltonetworks.com/new-hoaxcalls-ddos-botnet/

[4] 脆弱性対策の効果的な進め方 ツール活用編 テクニカルウォッチ IPA 情報処理推進機構（2020 年 5 月 13 日参照）
https://www.ipa.go.jp/topic/isec-technicalwatch-201902.html

«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