2018 年 3 月 27 日

サービス＆セキュリティ株式会社 e-Gate センター

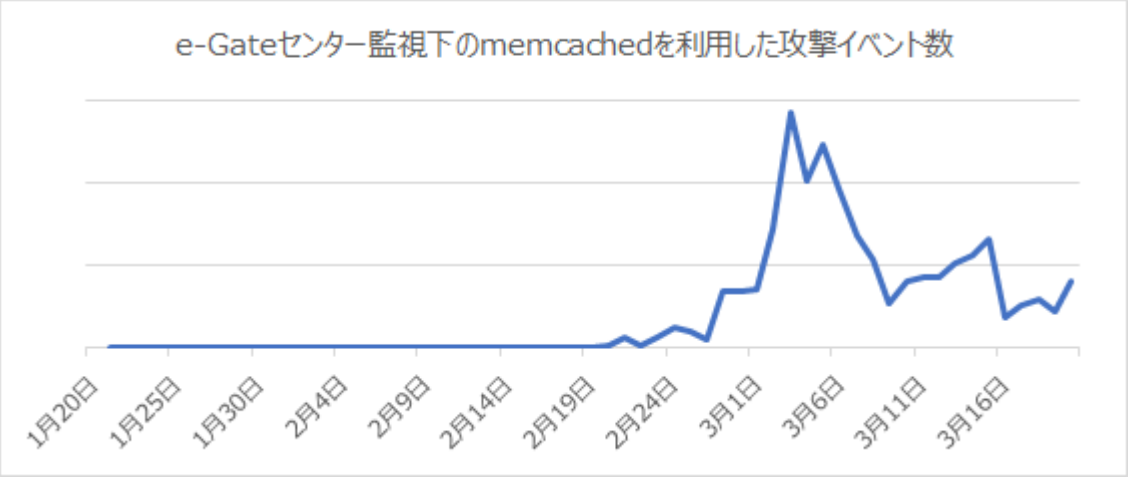
注意喚起：memcached を利用した DRDoS 攻撃について

1. 概要

2018 年 2 月 28 日、GitHub.com が DRDoS 攻撃（Distributed Reflection Denial of Service、分散反射型サービス不能攻撃）を受けて一時的にサービス不能となりました。memcached が稼働するサーバが反射攻撃を担うリフレクタとして利用され、ピーク時のトラフィックは 1.35Tbps に達したと報告されています。この攻撃は CVE-2018-1000115 として公開されている memcached の脆弱性を利用したものです。

セキュアソフトのグループ会社で 24 時間 365 日のセキュリティインシデント監視サービスを提供するサービス＆セキュリティ株式会社（以下、SSK）の e-Gate センターにおいても、同じ時期にリフレクタとして反射攻撃に加担させようとする通信を検知しています。下図は e-Gate センターが監視するシステムにおける当該通信のイベント数のグラフです。2 月 20 日頃からイベントが検知され始め、3 月 3 日にピークとなり徐々に減少していますが、依然として平常時よりも多くのイベントが検知されています。

攻撃の対象とされて被害を受けないようにするだけでなく、知らないうちに攻撃に加担させられ加害者とならないよう、対策を実施しなければなりません。正しい情報を把握して早期に対応することが必要です。



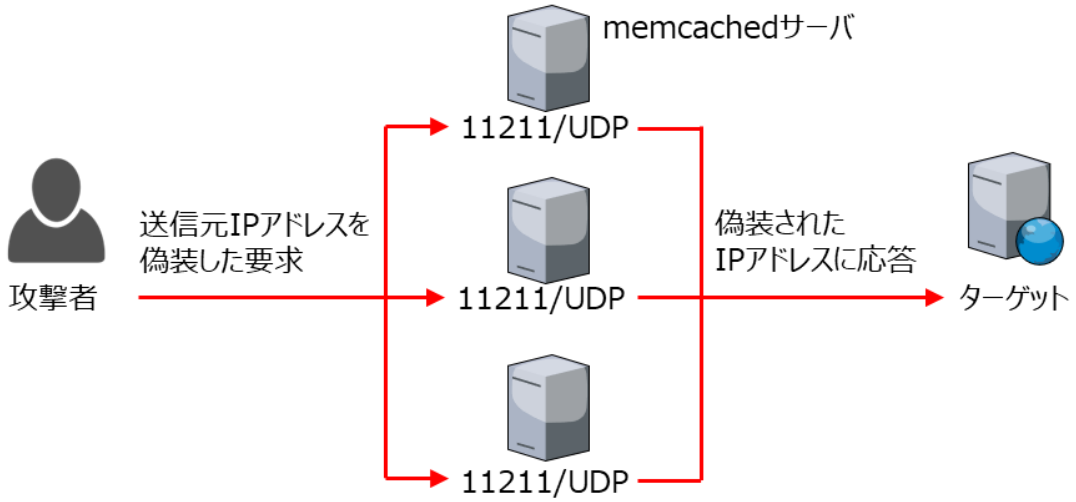
2. memcached を利用した DRDoS 攻撃と被害例

⑴ memcached とは

memcached は Web アプリケーションの高速化を目的に開発された分散型メモリキャッシュシステムです。memcached はデータをメモリ内に効率的にキャッシュする仕組みを提供します。その結果、データベースからデータを読み出す回数が減少し、Web アプリケーションの動作が高速になります。

⑵ memcached を利用した DRDoS 攻撃

下の図において、攻撃者はインターネット上の memcached サーバに対して、送信元 IP アドレスを攻撃対象の IP アドレスに偽装して、11211/UDP 宛ての要求パケットを送信します。これを受けたサーバは、攻撃対象の（偽装された）IP アドレスに応答パケットを送信します。



攻撃者が送信する要求が 1 パケットあたり数十バイトであるのに対して、memcached サーバの応答は 1 パケットあたり数百キロバイト程度にもなります。結果として、1 つの memcached サーバにつき、攻撃者が要求パケットを送信する通信帯域幅の 10,000～50,000 倍に増幅された応答パケットの攻撃を仕掛けることができます。更に DRDoS 攻撃（分散反射型サービス不能攻撃）においては、リフレクタ（反射攻撃を担うサーバ）の数だけ攻撃対象が受けるデータが増大します。

2018 年 2 月 28 日、GitHub.com は memcached を利用した DRDoS 攻撃を受け、17:21 から 17:30（いずれも UTC）まで全く利用できない、または一時的に利用できない状態に陥り、ピーク時においては 1.35Tbps のトラフィックを受けたと報告されています。

⑶ 対策

対策としては、memcached サーバの対策とネットワークの対策が考えられます。

① memcached サーバの対策：11211/UDP の利用制限・変更

memcached バージョン 1.5.5 以前では、既定で 11211/UDP が有効になっており、攻撃者に利用されました。11211/UDP のサービスが使用されていなければ、memcached の設定を変更して 11211/UDP を無効にしてください。2018 年 2 月 27 日にリリースされた memcached バージョン 1.5.6 では UDP を使ったアクセスが既定で無効となっています。

② ネットワークの対策：memcached サーバへのアクセス制限

memcached サーバからインターネットへの経路上にファイアウォールが設置されていることを確認してください。インターネットから memcached サーバへのアクセスは、特定 IP アドレスからの通信だけをファイアウォールで許可する、または必要がない場合は完全に遮断するなどして、memcached サーバへのアクセスを制限してください。

⑷ 参考情報

JPCERT/CC memcached のアクセス制御に関する注意喚起
https://www.jpcert.or.jp/at/2018/at180009.html

CVE-2018-1000115
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=2018-1000115

memcached バージョン 1.5.6 リリースノート
https://github.com/memcached/memcached/wiki/ReleaseNotes156

GitHub Engineering DDoS インシデントレポート
https://githubengineering.com/ddos-incident-report/

3. SSK、SecureSoft 製品・サービスの対応について

今回の攻撃は DDoS 攻撃の 1 種ですので、ターゲットとなるサーバの攻撃を緩和する為には、SSK のグループ会社であるセキュアソフトの次世代型 IPS 製品 Sniper ONE の DDoS 対策機能を活用することが有効な対策の 1 つとなります。また、攻撃を早期に発見する為に日々の運用監視が重要です。SSK の総合セキュリティサービス「e-Gate」監視サービスを活用頂くことで精度の高い検知、早期発見による迅速な事後対応が可能となります。

■SecureSoft Sniper ONE
ネットワークを通過するパケットに対して、様々な角度から詳細な分析を行い、攻撃を検知・遮断する事ができる「防御」のための不正侵入検知・防御システム（IPS：Intrusion Prevention System）です。Sniper ONE では DDoS 対策、RateLimit 機能などのオプションを用意しており、システムや想定する攻撃に合わせて DDoS 対策をおこなうことが可能です。

https://www.securesoft.co.jp/products/

■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。

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

※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。
※掲載した会社名、システム名、製品名は一般に各社の登録商標 または商標です。

«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