CloudCoffer

2020 年 3 月 3 日

セキュリティニュース：

マルウェアをシステムに埋め込む手法について 未対策の PHP は本当に危ない！

先の run.sh マルウェアの解析の中で、CloudCoffer 社解析チームはより詳細なインジェクションの手法についても追跡した。

ここでは、ペネトレーションテストやレッドチームオペレーションなど高度なセキュリティサービスを提供している関連会社である Ray Aegis Information Security ならびにその日本法人レイ・イージス・ジャパンの知見も加え、一般的に、どういう手法でこの種の攻撃が行われるのかを紹介する。

考えられる攻撃手法：

[1] アプリケーションレイヤーの OS コマンドに関する脆弱性やオブジェクトインジェクションの問題をついて埋め込む。（多くのアプリやデバイスの最新版でも脆弱性を含んでいる）

[2] PHP のゼロデイ脆弱性を突く （JPCERT/CC WEEKLY REPORT 2020-02-27 なども参照 ）

[3] アプリのアップロード機能を悪用する

[4] Shellshock 攻撃（本攻撃の詳細は Wikipedia の日本語版、英語版の記事などを参照されたい）

マルウェアの埋め込みは、そのほとんどがトロイの木馬方式で行われる。

現状での CloudCoffer 社による調査ならびに検知実績では、[2]の PHP からの侵入が多い。

CloudCoffer はどこで、どのようにマルウェアを検知したのか？

CloudCoffer 社の実施した POC において検出されたこのマルウェアとそれから派生したファミリーは、米国内のシステムに植え付けられ実行されていた。攻撃手法ならびに影響範囲の広さから、CloudCoffer 社としては今後も亜種が増えるものと予想している。

また、POC で使われていた CloudCoffer は通常版であり、Sandbox オプションは使わずに本マルウェアの通信を検知した。検知状況と通信内容によると、このマルウェア群は CloudCoffer により保護されていない他のシステムにも広く浸透していた、または浸透していったとみられる。

尚、このマルウェアに感染されているかどうかは、システムからのアウトバウンド通信でも判定可能である。攻撃者が侵害されたシステムを制御しようとして何らかの操作を行うとき、そのサーバー発の通信が発生する。

本資料作成時点で CloudCoffer が検知した実績として、攻撃者は DDoS を起動し、同時にマルウェアを植え付けようとしており、典型的な通信相手の IP アドレスとして次のものが使われている。

[1] 194.180.224.249

[2] 51.81.238.100

以上、少しでもご参考になれば幸いです。

ARIS Advanced Research & Information Service