2020 年 3 月 3 日

セキュリティニュース：

PHP からシステムが乗っ取られる？ ゼロデイ攻撃マルウェアを発見

CloudCoffer 社が実施する、CloudCoffer を利用した最近の Web セキュリティ実証実験（POC）において、PHP を使っている Web システムを丸ごと乗っ取る可能性のあるゼロデイ攻撃のマルウェアを検知した。

ゼロデイ攻撃（修正パッチや回避策などが提供されていない非常に初期の発見）となるため、CVE 番号などは本資料作成時点ではまだ付与されていない。

このマルウェア・ファイルはニックネームとして "run.sh"と呼ばれており、SHA-256 による ID は以下の通り。

SHA-256：

c8332368a2543088a36864c4dc708a1233ef56e20d1ccfc90ed5db5eec5a453e

本マルウェアは VirusTotal サイトにも登録されており、本資料作成時点（2020/2/27 時点、弊社調べ）では 9／58 個の製品が怪しい(malicious)ファイルとして検出している。検出対応数は徐々に増えてきている。

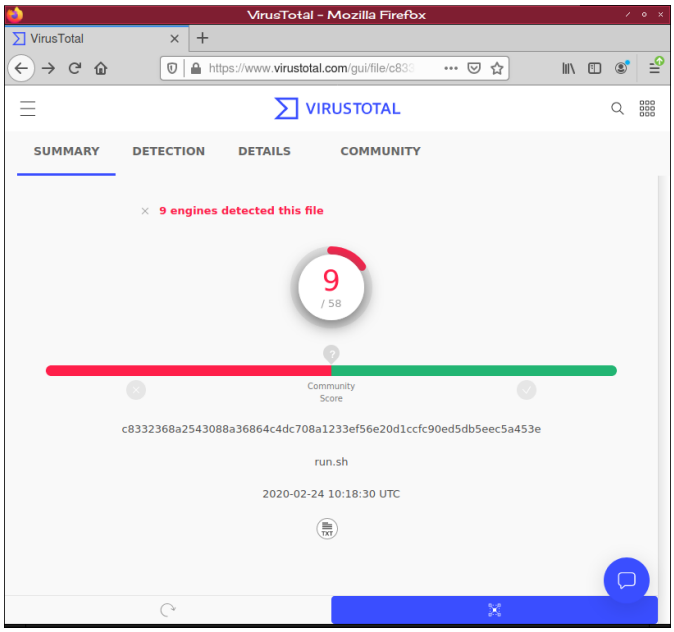

図 1 .Virus Total: run.sh(Summary)

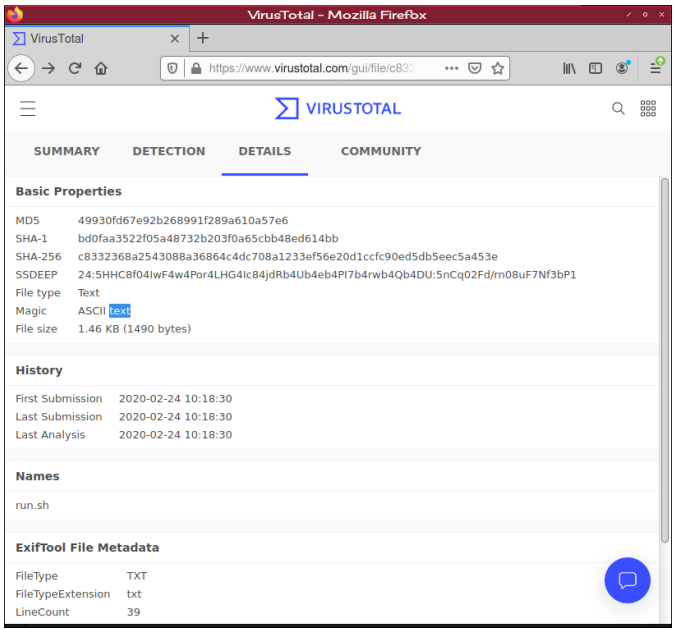

図 2 . Virus Total: run.sh(Detail)

本マルウェアについて、VirusTotal での初回登録日は 2020/2/24 である。

POC において、CloudCoffer は初回登録タイミングとほぼ同時に検知しており、検出結果を解析した内容について、株式会社アリスが CloudCoffer 台湾ラボチームから該当情報を得たのが 2020/2/26 だった。

つまり、CloudCoffer における「 **ゼロデイ攻撃の検知機能が証明された** 」と言える。

CloudCoffer はシグネチャベースの検知方式ではなく、A.I.で HTML ヘッダ／ボディを解析し、必要であれば多段階のデコード、復号化なども行って攻撃の判定を行う。

これによって、このマルウェアの攻撃が埋め込まれている HTTP 要求を自動検知した。（ログ情報は顧客希望により省略）

マルウェアの解析の結果概略は、以下の通り。

CloudCoffer での攻撃分類：

その他の分類（Un-categorized： これは、複数の分類にまたがる攻撃や複数の攻撃を組み合わせた攻撃手法が使われている、またはどれかを指定すると不正確になる、という理由で選ばれる分類項目）

エクスプロイト手法：

検知した情報だけでは特定できず、継続して注目している。エクスプロイトの一般的な手法について、別記事を用意しており、準備出来次第公開する。

マルウェアの機能や行動：

このマルウェアに感染すると、リモートから root／admin 権限のパーミッションを得ることができるようになる。

対象 OS として Windows と Linux に有効な攻撃である。攻撃用プロセスとして常駐し（ファイルレスであり、ディスクドライブ上のファイルスキャンでは見つからない）、外部からリモート制御する仕組みである。

ここまで侵されてしまうとシステムは攻撃者の思いのままになるので影響、被害は甚大である。

この攻撃への対策：

ゼロデイ攻撃なので、今後 CVE 番号が付与され、技術的内容が解析されたのち、各アンチウィルス、WAF のベンダーなどがシグネチャファイルの更新を準備、ユーザサイトで適用して初めて対策済み、となる。内容によって数か月遅れになるが、それまでの期間はいわゆる脆弱性期間となる。

一方 CloudCoffer は、その種のシグネチャファイルの仕組みを使っておらず、既に自動検知が確認できたので、この種の攻撃に対して非常に強力でメンテナンス・フリーなソリューションである。