2024年度

グローバル脅威レポート

年間レビュー

エグゼクティブサマリー

大規模言語モデル（LLM）の悪用から、自動化の利用の増加、攻撃の規模拡大、オープンソースツールの武器化に至るまで、2024年版のSysdig脅威レポートでは、クラウドベースの企業や組織が直面するアタックサーフェスの拡大と財政的負担について詳しく説明しています。

ランサムウェアのように経済的な大打撃を迅速にもたらす攻撃もありますが、多くの攻撃者は、より巧妙に立ち回ることで、長期間にわたって大きな損失をもたらす方法でリソースを吸い上げています。TRTがこの1年間を通じて報告した新たな脅威を詳しく調べることで、脅威のリアルタイム検知と迅速な対応の必要性を指摘する傾向が浮かび上がってきました。

賭けに出る

最新のAIがクラウドリソースを流出させる

2024年5月にSysdig TRTによって初めて確認されたLLMジャッキング（大規模な言語モデルを悪用するためのクラウドアカウントの窃盗）は、被害者に1日あたり10万ドル以上のリソース使用料を負担させる可能性があります。LLMジャッキングは、以前のクリプトジャッキングやプロキシジャッキングの手法を反映したものであり、リソースジャッキングにおける重要かつ高価な進化を意味します。

形勢を逆転させる

最善のツールを使って悪事を働く

Sysdig TRTは、今年、複数のオープンソースツールが武器化されたことを観測しましたが、中でもSSH-Snakeは、米国、中国、およびその他の国で認証情報の窃取を促進し、攻撃を拡大するものでした。オープンソースのSSH-Snakeツールのリリースから1ヶ月も経たないうちに、CRYSTALRAY脅威グループは、新しく作成された侵入テストツールを利用して、1,500件以上の被害者の認証情報を盗み出しました。

長期戦

ステルス性とパーシステンス

DDoS攻撃は、しばしば見過ごされがちです。なぜなら、DDoS攻撃はその影響力が過小評価されており、同攻撃を検知しそれに対応することが一般的に容易であると考えられているからです。RebirthLtdはDDoS-as-a-Service型のボットネットであり、ビデオゲームサーバー向けにマーケティングされています。RebirthLtdは一見無害であるように見えますが、それが提供する広範なアクセス権は、データ流出やスパイ行為につながる危険性があります。一方、よりステルス性の高いボットネットグループであるRUBYCARPは、防御回避を優先しており、Sysdig TRTが発見するまで10年以上も検知されないままでした。

リスクの高い賭け

市場トレンドに賭ける

先見の明があり、かつ金銭的な動機を持つ攻撃者たちが、市場トレンドと暗号通貨の予測に注目しつつ、正規のツールと盗んだアカウントアクセスを悪用して暗号資産Meson Network（MSN）を採掘していたことが判明しました。これは、MSNトークンがアンロックされる数ヶ月前に起こりました。MSNの価値が上がれば、このマイニングキャンペーンは大当たりとなります。

sysdig

EXEC-SUM-RP003-JA REV. A 10/24

レポート全文を読む →