2024年度

グローバル脅威レポート

年間レビュー

sysdig

目次

はじめに

Sysdig脅威リサーチチーム（以下「TRT」）は、『2023年度版グローバルクラウド脅威レポート』の中で、攻撃者が攻撃においてどのように進化し続け、どのようにクラウドサービスを活用しているかについて詳述しました。同チームは、サプライチェーンのセキュリティについて報告しているほか、攻撃者がクラウド環境で運用を行っている電気通信事業者や金融業界を優先的に標的としていることも明らかにしています。なお、『2023年度版グローバルクラウド脅威レポート』が明らかにした最も重要なことは、「多くの場合、クラウド攻撃は10分以内で実行される」という事実です。

サイバーセキュリティの状況は進化し続けており、サイバー軍拡競争において、攻撃者は手を緩めることがありません。Sysdig TRTは、2024年に起きたサイバー攻撃における重要な進化を観測しており、その特徴として、自動化の使用頻度の増加、攻撃の規模拡大、そして　リソース搾取の動機への継続的な移行を挙げています。今年は、自動化、オープンソースツール、そして最先端のテクノロジーを活用することで、収益の最大化とクラウドサービスの活用に重点を置き、リソースの搾取と新たな攻撃ベクターの両方を実現することを目指しています。その一方で、クラウド環境の特徴であるペースの速さは、Sysdig TRTの調査結果における中心的なテーマであり続けています。

今年Sysdig TRTが捕捉した攻撃の多くは、利益の創出か、もしくは高価なリソースへの無料アクセス権の獲得を動機としていました。LLMアクセスやクラウドアカウントなど、高価なリソースを利用して利益を得ようとする脅威は後を絶ちません。Check Point社によると、クラウドを利用した攻撃は前年比154%増となっており、クラウドにおけるスケーラビリティの容易さが理由で、攻撃者が大きな利益を得る機会が増えています。

多くの企業や組織にとって、2024年は経済的負担の多い年でした。損害が年々高額化しているだけでなく、攻撃者が被害者に課すコストも天文学的な数字となっています。これは、最新の攻撃が備えている高度なスケーラビリティと迅速さが原因です。

下記のレポートでは、Sys-dig TRTが2024年に発生した最も新しい脅威アクターと攻撃キャンペーンから得た調査結果を紹介しています。

攻撃は10分以内で実行される

「**クラウドの検知と対応における555ベンチマーク**」を通じて、クラウド攻撃に打ち勝つ方法を学ぶ

今すぐ読む →

DRAIN ON RESOURCES

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により初めて特定されたLLMジャッキングは、大規模言語モデル（LLM）を悪用するためにクラウドアカウントを窃取しようとする攻撃であり、この攻撃は当初、被害者に1日あたり最大46,000ドルの損害を与えるものと見られていました。しかし、6ヶ月前まで遡ると、モデルの進化と価格の上昇が理由で、被害者は1日あたり10万ドル以上の損害を被る可能性があることが判明しました。LLMジャッキングは、過去に存在した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ていますが、より手ごわい経済的脅威をもたらし、リソース乗っ取りにおける重要な進化を示すものとなっています。

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件以上のユニークな認証情報を盗み出しました。

USED FOR EVIL

PERSISTENCE

長期戦

ステルス性とパーシステンス

分散型サービス拒否（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、新たな標的を攻撃する

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。しかし、MSNの価値が上がらない場合、このマイニングキャンペーンはリスクばかりで見返りのないものとなります。

NEW TARGETS

リソース悪用における新たなフロンティア

LLMjacking

クラウドアクセスやクラウドホステッド型のリソースは、非常に高価であり、かつ非常に高速です。このため、そのようなリソースは、アクセス権を入手するか、またはアクセス権を販売して利益を得ようとする攻撃者にとって格好の標的となっています。Sysdig TRTは以前にも、無料アカウントのトライアルからプロキシサービス、そして今回のLLMに至るまで、さまざまなリソース乗っ取りについて報告してきました。Sysdig TRTでは、金銭的な動機に基づくLLMジャッキングだけでなく、インターネットアクセスが制限されている国や、アクセスを完全にブロックするような制裁措置が取られている国からのLLMジャッキング攻撃も確認しています。このようなケースでは、悪意あるアクセスや盗まれたリソースが、これらの国の居住者が制限を回避してグローバルなインターネットリソースに接続するための手段となります。

脅威の詳細

大規模言語モデル（LLM）は、ほぼすべての業種に革命を起こしていますが、その一方で、それは大きな代償をもたらしています。Sysdig TRTは2024年5月に、LLMを悪用した攻撃である**LLMジャッキング**について初めて報告しました。攻撃者は、盗んだクラウド認証情報を使用して被害者の環境へのアクセス権を入手すると、クラウドホステッド型のLLMへのアクセス権を特定しました。

これらの攻撃は金銭的な利益を動機としている可能性もありますが、より重要なのは、これらの攻撃がLLMリソースへのアクセス権を無料で提供したことです。

LLMジャッキングは、プロキシジャッキングやフリージャッキングに似ています。攻撃者は、多くの場合コストのかかるリソースへのアクセス権を得ようとします。攻撃者は、アクセス権を盗むことで、国家によるブロッキングや制裁が理由で入手できないかまたはアクセスできないようなツールやプロファイルに無料でアクセスできるようになります。LLMリソースの中には、ロシアのような国では制裁措置の対象となっており、アクセスできないものもあります（Bedrock、Anthropic、Open-AIなど）。また、中国や北朝鮮では、一部のWebサイトへのアクセスが制限されています。このような事情が、これらの国に居住する人々を不正な手段でアクセス権を得るように駆り立てている可能性もあり

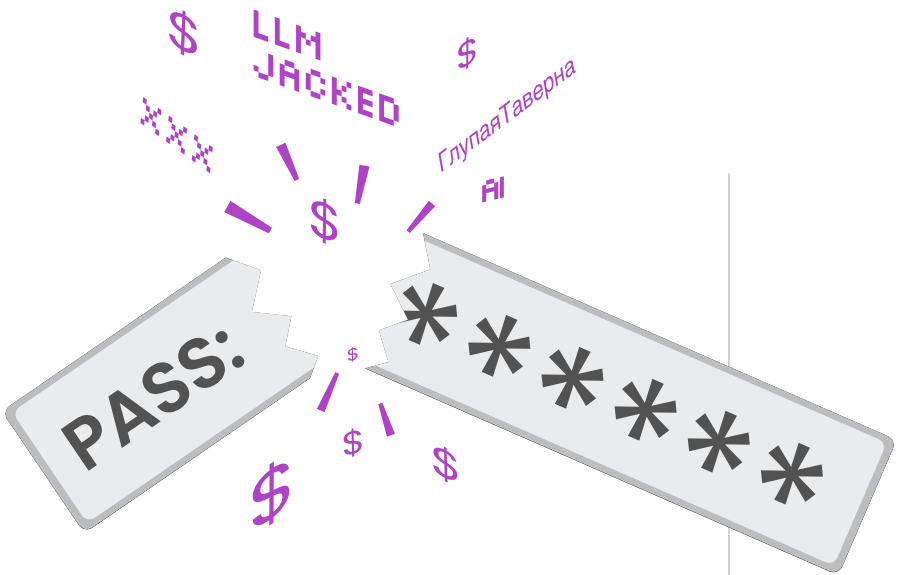
フリージャッキング

- **Sysdig TRTが、GitHub Actionsを活用した大規模なクリプトマイニングを発見**
- **GoogleのAIプラットフォームであるVertexがフリージャックされる**
- **AWSの隠れた脅威：クラウドネイティブクリプトジャッキング攻撃**

プロキシジャッキング

- **プロキシジャッキングがチャットに登場**
- **LABRAT：GitLabを標的としたステルス型のクリプトジャッキングとプロキシジャッキング攻撃**

STOLEN ACCESS



LLMおよびプロキシサービスのようなリソースやツールは、高価なものとなる可能性があります。最初のLLMジャッキング攻撃において窃取された企業のアクセス権は、ローカルなAnthropic Claude 2.xモデルのアクセス権でした。この攻撃で、被害者は1日あたり46,000ドルものコストを負担することになりました。より新しいClaude 3.5 Opusバージョンでは、1日あたりのコストが2倍から3倍になる可能性があります。

攻撃者のアクセス権が削除されるまで、LLMの不正利用は止むことがありませんでした。たとえば、1人のLLMユーザーが1日に500件から1,000件、あるいはそれ以上のコールを行う可能性があります。しかし、7月に、LLMアクセス権が共有または販売されており、かつ自動化が使用されているという前提の下で、Sysdig TRTは、3時間で80,000件もの大量のコールが行われたのを目撃しました。これは、被害者にとって、わずか**3時間**で約24,000ドルから30,000ドルの請求額が発生したことを意味します。

クリプトマイニングの場合、CPUリソースの消費量の増加は、特定の振る舞いに基づいて簡単に特定が可能であり、即座にアラートをトリガできます。しかし、LLMの利用は、LLMへの呼び出しという1つの振る舞いしか存在しないため、このような方法では検知できません。LLMリソースの消費量は、個々のユーザーによって大きく異なるため、正当な使用と不正な使用を区別することは困難です。

たとえば、お使いの企業環境でAWS Bedrockを通常見かけない場合、その利用は疑わしいものとなります。また、AWS Bedrockを 1 つのリージョンでのみ利用している場合に、その利用が別のリージョンで見られたならば、その利用は疑わしいものとなります。使用量が10倍（またはその倍数）に増えた場合、その利用も疑わしいものとなるため、調査が必要となります。セキュリティチームが使用量の異常な急増をすぐに特定できるようにするには、何が正常な振る舞いであるかを知ること、そして自社のクラウドアカウントにおけるLLM使用量の基準を確立することが不可欠です。

LLMジャッキング攻撃により被害者が負担する可能性のある費用

1日あたり

$100,000

使用ツール

Keychecker
指定されたLLMで使用される認証情報を検証

OAIリバースプロキシ
窃取された認証情報とLLMを使用して、認証情報の制御を維持しつつアクセス権を提供

ハッカーが悪意を持ってOSSを利用

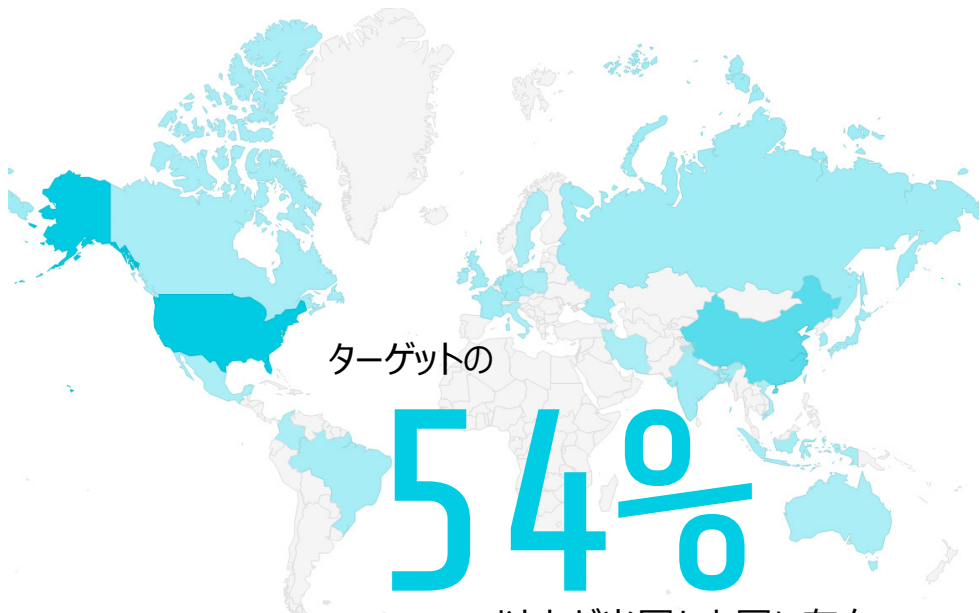
CRYSTALRAY

オープンソースソフトウェア（OSS）のセキュリティ対策ツールは、インターネットに接続できるならば世界中の誰もが無料で簡単に利用できます。OSSセキュリティツールは、防御者の仕事をより速く、より簡単に、より正確にすることを意図しています。その一方で、攻撃者は悪意を持ってOSSを利用しています。防御者は、企業ユーザーが信頼できるOSSツールをダウンロードして利用しているのを見たとしても、それについて深く考えない可能性があります。これは、攻撃者にとって完璧な隠れ蓑となります。

脅威の詳細

Sysdig TRTは、新しく開発したOSS侵入テストツールSSH Snakeを使用して、2024年2月に**CRYSTALRAY**脅威アクターを初めて特定し、その後数ヶ月にわたって同脅威アクターが攻撃を強化するのを監視し続けました。Sysdig TRTは7月に、この脅威アクターが保有しているツールスイート全体に関する**最新情報を含むブログ**を公開しました。

2月から7月にかけて、CRYSTALRAYの被害者数は当初の10倍となる1,500件を超えました。標的となったIPアドレスの54%以上が、米国と中国に割り当てられているものでした。下記の地図は、グローバルな攻撃対象の内訳を視覚化したものであり、最も頻繁に標的とされている国としては、北米（38%）、アジア（29%）、そしてヨーロッパ（11%）が挙げられます。これらのリージョンが標的とされている理由としては、オープンポートの数が多いことや、既知の脆弱性が放置されていることが考えられます。



標的となった国

米国	36.4	フランス	2.5	カナダ	1.2	メキシコ	0.6	ベトナム	0.5
中国	17.9	インド	2.4	アイルランド	0.9	台湾	0.6	コロンビア	0.4
ドイツ	3.5	韓国	2.4	オーストラリア	0.8	チェコ	0.6	イタリア	0.4
シンガポール	3.5	英国	2.1	イラン	0.8	ポーランド	0.5	バングラディシュ	0.3
ロシア	2.7	ブラジル	1.6	オランダ	0.7	スウェーデン	0.5	その他	5.6
日本	2.5	インドネシア	1.4						

CRYSTALRAYキャンペーンの持つ洗練性は、ブラックマーケットにおける認証情報の収集と販売において目新しいものです。この脅威アクターは完全なOSSツールスイートを悪用することで、自分たちのゲームを自律的に拡大し始めました。Sysdig TRTは、このキャンペーンに関連している可能性のある、1つ20ドルで販売されている認証情報を特定しました。しかし、被害者が受ける影響はさらに大きくなる可能性があります。認証情報が売られた後、被害者に何が起こるかは、現時点では何も分かっていないからです。

おそらく、Sysdig TRTがCRYSTALRAYの脅威の手口を公表したためと思われます　　が、同グループは7月にブログを公表した後、その活動を停止しました。本稿執筆時点では、Sysdig TRTは新たなCRYSTALRAYキャンペーンを特定していません。CRYSTALRAYのように、一部の脅威グループは、公衆の面前で見世物にされることや、法的処分を受ける可能性があることに怯えています。脅威の調査において、さらなる悪意ある行動を抑制する最良の手段の1つとして、脅威の全容を暴露することが挙げられます。

CRYSTALRAYキャンペーンの持つ洗練性は、ブラックマーケットにおける認証情報の収集と販売において目新しいものです。

使用ツール

pdtm
ProjectDiscoveryツールスイートの管理と保守

SSH-Snake
SSHベースのワームであり、ネットワークをマッピングして認証情報を収集する

ASN
インターネット全体を通じてネットワークデータを偵察

zmap
ネットワーク偵察およびサービス検出ツール

httpx
Webサーバーをマッピングするhttpベースの高性能スキャナー

nuclei
オープンソースの脆弱性スキャンツール

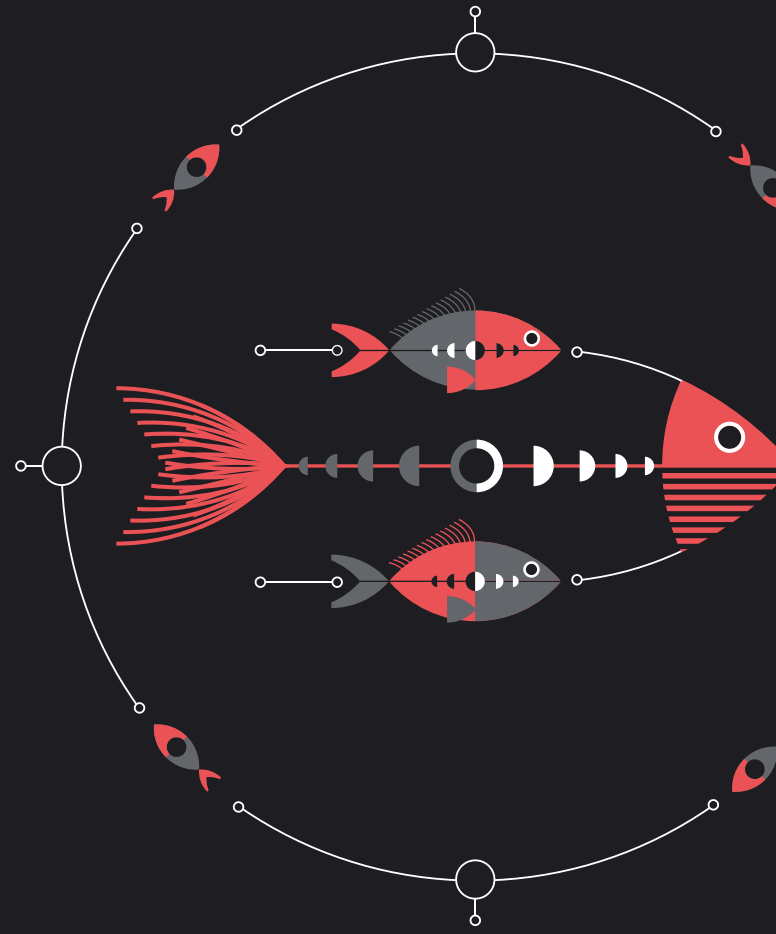
Sliver
Cobalt Strikeに似たパーシステンスおよびリモートアクセスツール

Platypus
パーシステンスと被害者のアクセス管理

より高い洗練性、持続的な成功

RUBYCARP

防御の回避、パーシステンス、そしてステルス性は、ほぼ同義語であり、攻撃を成功させるための礎となるものです。攻撃者が身を隠す時間が長いほど、より多くの金銭とインテリジェンスを集める機会が増えます。傲慢さをうまく抑え、ツール、ステルス性、能力を進化させることができる脅威アクターは、より長い期間、無傷で金銭を稼ぎ続けることができます。ステルス性の高い高度な持続的脅威（APT）は、何年にもわたって潜伏してデータを収集するか、またはデータを流出させることが知られています。多くの攻撃者にとって、毎月数100ドルの収入が得られることは、気の長いアプローチを採用するのに見合う価値があります。



RU CA BY RP

脅威の詳細

2024年4月、Sysdig TRTはあるボットネットグループを発見しました。**RUBYCARP**と名付けられたこのボットネットグループは、少なくとも10年間は手付かずのまま運用されていたようです。なぜこの10年間、このグループに対する法的措置が取られなかったのでしょうか？その理由は、おそらくオープンソースの帰属を明らかにすることが非常に難しいからでしょう。Sysdig TRTが特定したperlスクリプトであるshellbotについては数百件もの報告がありますが、このツールの背後にいる人物についての報告は一切ありません。

しかし、近年では、**9年間にわたって稼働していたルーマニアのボットネット**が報告されているほか、直近では3年間だけ稼働していたルーマニアのボットネットが報告されています。おそらく、このようなボットネットグループは検知を回避するのが得意なのでしょう。結局のところ、クリプトマイニングのセットアップログを保存するために使用された主要ドメインは、ブルガリアの化学技術冶金大学のサブドメインであるphysics. uctm[.]eduでした。

RUBYCARPのメンバーは、防御者が検知していると推測できるような既知のツールの拡張的なスイートを構築するのではなく、キルチェーンに必要なものの多くを10年間にわたってカスタマイズし、定期的に更新することで、検知されるリスクを低減しました。

さらに、RUBYCARPボットネットグループは複数の異なる脆弱性を標的とすることで、潜在的な被害者プールを拡大し、その攻撃の検知を最小限に抑えていました。当初報告されていた脆弱な Laravelアプリケーション（CVE 2021 3129）に加えて、彼らは Alibaba Cloud、脆弱なGitLab Community、そしてEnterprise Edition サーバー（CVE 2021 22205）も標的としていました。

RUBYCARPは、金銭的な動機で活動している成功したボットネットグループです。あるメンバーは、わずか1日で360ドル（1,600ルーマニアレイ（RON）以上に相当）を稼ぎました。また、Sysdig TRTは2年間活動しており、その間に22,800ドル（100,000 RONに相当）以上を稼いだメンバーのウォレットを特定しました。TRTは、このような利益を得ているウォレットが他にも多く存在していると確信しています。特にルーマニアの物価を考慮するならば、そのようなケースは今後さらに増えると思われます。

使用ツール

Banner
ポートスキャナーツール

Masscan
一般的なネットワーク検出ツール

X kernel module
ファイルやプロセスを隠すために使用される

Brute
カスタムSSHブルートフォースツール

Shellbot
IRCサーバーにジョインするためのPerlスクリプト

IRCサーバー
チーム全体での通信に使用されるほか、各キャンペーンの詳細情報を保存するための作業用フォルダとして使用される

C3Bash
カスタムのコマンドラインマイナーのセットアップを行う

少なくとも

10年間

は手付かずのまま運用されていたようだ

過去10年間、なぜこのグループに対する法的措置が取られなかったのか？

攻撃者は、あなたが利用しているサービスを狙っている

REBIRTH

成功した企業は、合理的で反復可能な営業活動が成功の鍵であると言うでしょう。起業家精神にあふれた脅威アクターについても、これと同じことが言えます。脅威アクターがDDoSのような成功した攻撃を構築し自動化することができれば、彼らはより多くの攻撃やサービスを提供し続けることが可能となり、リピート顧客を増やすことができます。一部の攻撃グループの背後にはマーケティングエンジンが存在しており、彼らの成功は意図的な努力の上に成り立っています。

脅威の詳細

分散型サービス拒否（DDoS）攻撃は、しばしば見過ごされがちです。なぜなら、DDoS攻撃は大げさに宣伝されてはいるものの、通常は簡単に修復できるためです。しかし、DDoS攻撃が終わった後、それがあなたの組織に痛みを与えていないように見えたとしても、攻撃者は今もなおアクセス権を保持している可能性があります。この種の攻撃は、他の悪意ある活動から被害者の目をそらすためのものであり、被害者をデータ流出やスパイ行為、あるいはそれ以上のリスクにさらす可能性があります。攻撃手法を変更することは困難で時間がかかるため、攻撃者は必要な場合を除き、必ずしもその手法を洗練させるとは限りません。DDoS攻撃は依然として効果的な攻撃手法であり、今年も**Microsoft** Azureのグローバルインフラが数時間にわたってダウンした際に観測されました。

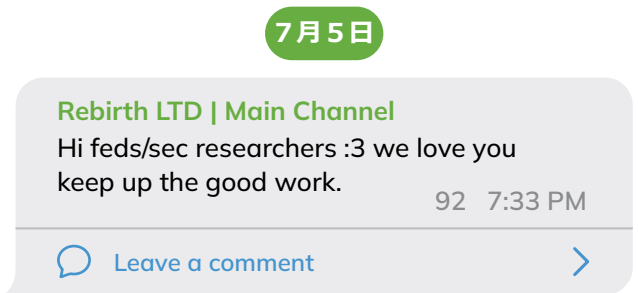
2024年3月、Sysdig TRTは、Miraiマルウェアのソースコードから開発された**RebirthLtd**と呼ばれるDDoS-as-a-Serviceボットネットを発見しました。同グループはビデオゲームサーバー向けに自らのDDoSサービスをマーケティングしていますが、同サービスがゲームサーバー以外のターゲットにも使用できないとは言い切れません。

RebirthLtdボットネットが販売された場合、そのアクセス権を利用して何が可能となるかは分かりません。

BOTNET FOR SALE

一度売られたら、アクセス権は何にでも使用できます。より重要なことは、RebirthLtdボットネットの動作を評価し理解した上で、それに対する防御を行うことで、より破壊的な他のDDoS攻撃に対する防御セキュリティを改善できるということです。

Sysdig TRTは、2019年の初期テスト段階から、今年1月に開始された現在の広告販売に至るまで、RebirthLtdグループによるサービスの開発を明らかにしました。同グループは、ボットネットの使用料として15ドル～53ドルを請求しています。費用は、アクセス、サポート、能力のレベルにより異なっています。Sysdig TRTでは、RebirthLtdの脅威アクターが今年の初めにTelegram経由のマーケティング活動を開始して以来、ささやかな副収入を得ていると推測しています。



Sysdig TRTが3月にRebirthLtd関連の記事を発表した後に送られてきたTelegramのメッセージ。

使用ツール

Mirai
このボットネットの構築に使用されたマルウェアのソースコード

QBotおよびSTDBot
バックドアの確立に使われるマルウェア型トロイの木馬

各種のエクスプロイトツール
バックドア用NETISルーター、http攻撃用ユーザーエージェントリスト、Telnet/SSH用IPスキャナー、ブルートフォース攻撃

tcpfloodおよびudpflood
DDoS機能を提供し、ジオブロッキングを制限

マーケットドリブン型の攻撃

Meson暗号資産CDN

金銭的な動機に基づいて活動する脅威アクターは、悪意あるギャンブルで最大の報酬を得ることに投資しています。クラウドプロセスと自動化は、攻撃者が標的にたどり着く能力を強化します。攻撃者は、より迅速に作業し、かつより容易にスケーリングできるようになるほど、より多くの利益を得ることができます。金銭的に動機を持つ攻撃者は、より多くの利益を得るために、面倒なプロセスを自動化しています。

脅威の詳細

ハッカーは新しいテクノロジーをいち早く採用し、新たな機会を狙っています。2024年2月、**ある攻撃者**は、新たな暗号資産トークンのアンロックを予期して、そのトークンに価格がつく前に自らの活動を活発化させました。Meson Network（MSN）はWeb3上のブロックチェーンプロジェクトであり、Google DriveやAmazon S3のような、より高価な従来のクラウドストレージソリューションに取って代わることを意図しています。

被害者の環境にアクセスしてから数分以内に、攻撃者はハッキングしたクラウドアカウントを使用して6,000ノードの作成を試みました。このプロセスは自動化されており、1リージョンあたり500マイクロサイズのEC2インスタンスの各バッチを起動するのに約20秒かかりました。マイクロサイズのノードでは、6,000ノードで1日あたり2,000ドルのコストがかかりますが、パブリックIPアドレスでは1日あたり22,000ドルになります。被害者である企業が作成可能なノード数を制限しない限り、攻撃者は可能な限り多くのノードを作成し続けるでしょう。これらの試算を超えた場合、被害者が負担する費用は天文学的な数字になる可能性があります。

攻撃者は、ロックされた暗号通貨を採掘する準備を整えることにより、金銭的な利益を得られる可能性に賭けていました。MSNコインはCPUに基づいて採掘されるわけではないため、この操作により攻撃者が得ることのできる金銭的成果を計算するのは困難です。上記のコストを計算するのに使用した計算式は、いくつかのスコアに基づいています。また、2月にこの攻撃が発生した際のMSNの価格は約4.60ドルでしたが、5月にこの暗号資産トークンが発売されると、その価格は大幅に下落しました。それ以来、MSNの価格が1ドルを超えることはありません。このような状況では、将来の大儲けを計画したとても報われなかったことでしょう。

使用ツール

この攻撃では、公式**Webサイト**から直接ダウンロードして実行されたMSNマイニングソフトウエア以外に、ツールは使用されていません。

ハッカーが被害者にもたらす可能性のあるコスト

1日あたり

$22,000

要点と今後の予想

サイバーセキュリティは常に進化しており、クラウド環境ほどそれが顕著に当てはまります。過去2年にわたって当社が報告してきたように、脅威アクターやサイバー攻撃者はイノベーションを実現し自らの攻撃を成功させることに専心しています。これは、私たちが攻撃者から身を守ることに専心しているのと同じです。

2025年、攻撃者は、より迅速かつ大規模なデータ流出、情報収集、金銭的利益を得るために、キルチェーンを迅速化するタスクを自動化し続けることが予想されます。また、攻撃者は同じ理由から、新しい革新的なテクノロジーやツールをターゲットとし、それを使用することで、攻撃の成功率を高めることが予想されます。AIは未来を切り拓くテクノロジーです。私たちは2024年にAIサイバーセキュリティ闘争の初期段階を目撃しましたが、2025年にはさらに多くのことが起こるでしょう。LLMジャッキングはAIに対する新たな脅威の始まりに過ぎず、今後12ヶ月の間に、脅威アクターがAIを使用して自らの攻撃を強化するであろうことも容易に予想されます。

1 スケーラビリティ

クラウド環境ではスケーリングが容易であるため、2025年にはDDoS攻撃の割合が増加するでしょう。サービス拒否は企業規模での大規模なパニックを引き起こすため、攻撃者が被害者のネットワークにより深く侵入している間に、被害者の目をそらすことができます。

2 アタックサーフェス

特にLLMがすべてのセクターで使用されるようになると、アタックサーフェスは来年以降も拡大し続けるでしょう。かつて区分けされていたデータは、より高い生産性を実現するために一元化され、LLMへとフィードされ続けるでしょう。ただし、大量のデータをLLMに押し込むことで、新たな集中リスクを生み出し、アタックサーフェスを拡大し、攻撃者のためのチャンスを増やすことになる場合もあります。

3 自動化

LLMの台頭は攻撃の成功に貢献するでしょう。2025年には、攻撃者はオーディオクローンやビジュアルクローンを使って、MFAを標的とすることに成功するでしょう。その一方で、攻撃者が状況を把握し、LLMの内部動作を理解し続ける中で、プロンプトエンジニアリング攻撃が増加することが予想されます。

4 コスト

攻撃による企業の被害コストは増加すると予想されます。**IBMによると**、2024年の侵害の平均コストは468万ドルです。しかし、パブリッククラウドの侵害の場合、この数字は517万ドルに増加します。米国だけでも、2024年上半期に**報告された情報漏洩**の件数は1,500件を超えています。これらの予測を考慮すると、2025年の世界的なサイバー攻撃の被害額は1,000億ドルを超えると予想されます。

> **攻撃者の防御回避手段は成熟の一途をたどっているため、単に攻撃を防ぐだけでは十分ではありません。**
>
> 脅威リサーチ部門シニアディレクター
> **Michael Clark**

プロアクティブなセキュリティプログラムは、常にハッキングを前提とすべきです。攻撃者の防御回避手段は成熟の一途をたどっているため、単に攻撃を防ぐだけでは十分ではありません。強力なリアルタイム検知と迅速な対応は、防御者が未知の攻撃を特定し阻止するのに役立ちます。サイバー攻撃に対するレジリエンスは、ビジネスを継続させるのに役立つでしょう。

クラウド攻撃は年々、より速く、より巧妙に、そしてより高価なものになっていくでしょう。

Sysdig脅威リサーチチーム

Sysdig脅威リサーチチーム（TRT）は、クラウドやコンテナ環境、ランタイム、および脅威検知に特化した脅威リサーチの最先端で仕事をしています。TRTは熟練した研究者たちにより構成されたグループとして知られています。TRTは、クラウド攻撃が10分間で実行されるという事実を最初に報告したほか、クラウド脅威の検知と対応のための555ベンチマークを設定し、さらに**PURPLEURCHIN**や**SCARLETEEL**などの新しい脅威を発見しました。また、TRTは、Dock-erHub、GitLab、AWSなどの防御ツールを武器にした大規模なクリプトマイニングキャンペーンやボットネットをいくつも発見しています。

Sysdig TRTは、クラウドとコンテナに関する脅威状況を追跡しているほか、SysdigとFalcoの検知アナリティクスの開発と改善、さらには研究結果についてセキュリティコミュニティを教育するコンテンツの制作と配信を行っています。2021年にチームが設立されて以来、Sysdig TRTはオープンソースのFalcoコミュニティ向けに500以上の検知ルールを作成してきました。脅威インテリジェンスフィードとカスタマイズされたハニーポットに加えて、TRTはMLとAIのアルゴリズムを利用して、Sysdigの脅威検知ルールと機能を改良しています。

Sysdig TRTに所属している熟練したセキュリティ専門家は、世界中に分散しています。同チームのメンバーは、政府機関、民間企業、学術機関などでの多様な経験を有しており、攻撃および防御のセキュリティオペレーション、コンピュータネットワークオペレーション、マルウェア解析などの専門知識を有しています。同チームのメンバーは、BlackHat、RSA、fwd:cloudsec、KubeConなど、世界中の大小さまざまなイベントに定期的に参加しています。

TRTからの新着情報

最新のクラウド脅威に関するリサーチ、トレンド、ベストプラクティスについては、Sysdig脅威リサーチチームのリソースセンターをご覧ください。

さらに詳しく →

Falco

Falcoは、分散されたインフラストラクチャー全体に導入できるセキュリティカメラのネットワークのようなものです。Falcoは、ランタイムセキュリティに基づいて、あらゆる環境におけるリアルタイムの検知、監視、および可観測性を提供します。Falcoは、Kubernetes、Linux、およびクラウド向けに特別に構築された、すぐに使えるセキュリティルールセットを提供します。Falcoは、コミュニティ主導型のオープンソースソフトウェアです。2021年以来、Sysdig TRTは、Falcoコミュニティのために500件を超える数の検知ルールを作成してきました。

Sysdigについて

クラウド環境では、1秒1秒が重要となります。攻撃は驚くほどの速さで進行するため、セキュリティチームはビジネスを減速させることなく、攻撃から守る必要があります。Sysdigは、ランタイムインサイトとオープンソースのFalcoを利用することで、リスクにおける変化を即座に検知し、クラウド攻撃をリアルタイムで阻止します。Sysdigは、クラウドのワークロード、アイデンティティ、サービス全体におけるシグナルを相互に関連付けることで、隠れた攻撃経路を明らかにすると共に、真のリスクに優先順位を付けます。予防から防御に至るまで、Sysdigは企業がイノベーションという最重要事項に集中できるよう支援します。

さらに詳しく →

sysdig

REPORT

RP-010-JA REV. A 10/24