Press Release
報道関係各位

SecurityScorecard株式会社
2025年7月8日

SecurityScorecard
世界規模のスパイ活動を支える中国の新型ORBネットワーク「LapDogs」に関する調査レポートを発表
-グローバルに拡大するステルス性の高いスパイ活動を分析-

SecurityScorecard株式会社（本社：米国、ニューヨーク州、CEO：アレクサンドル・ヤンポルスキー、以下SecurityScorecard、日本法人代表取締役社長　藤本 大）は、同社の脅威分析チーム「STRIKE」の最新調査レポート、「**LapDogs：世界規模のスパイ活動を支える中国の新型ORBネットワーク**」を公開しました。本レポートでは、これまで明らかにされていなかった ORB（Operational Relay Box) ネットワーク「LapDogs」 を特定し、その実態を詳細に分析しています。「LapDogs」は、中国のサイバー攻撃者が活用する長期的かつステルス性の高いスパイ活動キャンペーンの基盤です。

主な調査結果

- 世界で**1,000以上の感染ノード**を確認
- **日本を含む**東南アジアと米国に標的が集中。主に被害を被った業界は**不動産、IT、ネットワーキング、メディア**など多岐にわたる
- 「LapDogs」は“ShortLeashと呼ばれるカスタムバックドアを活用し、デバイスに侵入・常駐、攻撃者が目立たずに活動できる環境を構築
- 主な標的はSOHO（小規模オフィス/ホームオフィス）で利用されているデバイス
- キャンペーンは**2023年9月から計画的かつ段階的に拡大**
- 「PolarEdge」など中国と関係する既存ORBネットワークとの類似点を持つ一方、独自の構造と挙動を有するため、明確に区別

背景

近年、ORBネットワークは、国家支援型の脅威アクターによって使用される**極めて効果的かつ秘匿性の高いインフラ手法**として静かに台頭してきました。従来のボットネットとは異なり、ORBは目立った攻撃を行うのではなく、侵害されたデバイスを用いて長期間にわたり秘匿インフラを維持します。これにより、悪意ある活動の隠れ蓑として柔軟に機能し、感染したデバイスは通常通り動作するため、検出および追跡が非常に困難です。

ORBネットワーク「LapDogs」は遅くとも2023年9月から活動を開始し、それ以降、世界中で活動を拡大しています。攻撃者は“ShortLeash”というカスタムバックドア型マルウェアを利用してデバイスに侵入し、相互接続されたネットワークを構築。バックドアは、「LAPD（米ロサンゼルス市警）」を装った自己署名型TLS証明書を生成しており、これはロサンゼルス市警察を模倣することで偽装しようとする試みと見られます。

セキュリティチームへの警告

我々の調査により、これらの証明書が世界中の1,000以上の感染ノードに紐づいていることが判明し、構造化された攻撃任務に基づく地理的ターゲティングが明らかとなりました。証明書の生成パターンには、地域ごとの小規模侵入キャンペーンに連動したスパイクが確認されており、たとえば日本、台湾など特定の地域に対して集中的な攻撃を行っている様子が見られました。これらは単発的ではなく、計画的かつ波状的に展開された侵入作戦であり、LapDogsが明確な意図を持つターゲット志向型のアクターであることを裏付けています。従来のIOC（侵害の兆候）ベースの対策だけでは脅威アクターの特定や対応が困難になる恐れがあり、包括的な脆弱性管理とネットワーク監視の重要性がますます高まっています。
SecurityScorecardは今後も、世界規模のサイバー脅威に関する透明性を高め、企業・政府機関の防御態勢強化を支援していきます。

レポート全文は、こちらを参照ください（英語のみ）

SecurityScorecard のThreat Research, Intelligence, Knowledge, and Engagement (STRIKE) チームについて
独自の脅威インテリジェンス、インシデント対応の経験、サプライチェーンのサイバーリスクに関する専門知識を兼ね備えています。SecurityScorecardのテクノロジーに支えられたSTRIKEチームは、世界中のCISOの戦略的アドバイザーとなり、STRIKE チームによる脅威調査を基に、組織にサプライ チェーンのサイバー リスクと攻撃者の特性に関してアドバイスを行っています。

SecurityScorecardについて
Evolution Equity Partners、Silver Lake Partners、Sequoia Capital、GV、Riverwood Capitalなど、世界トップクラスの投資家から出資を受けたSecurityScorecardは、サイバーセキュリティ レーティングにおけるグローバルリーダーであり、Supply Chain Detection and Response（SCDR・サプライチェーンにおける検知・対応）ソリューションのパイオニアです。
セキュリティとリスクの専門家であるアレクサンドル・ヤンポルスキー博士とサム・カッスーメによって2013年に設立されたSecurityScorecardの特許取得済みセキュリティレーティングテクノロジーは、企業のリスク管理、サードパーティリスク管理、取締役会報告、デューデリジェンス、サイバー保険の引き受け、規制当局の監視のために25,000以上の組織で使用されています。
SecurityScorecardは、企業におけるサイバーセキュリティ・リスクの理解、改善を促進し、取締役会、従業員、ベンダーに伝える方法を変革することで、世界をより安全にすることを目指します。https://jp.securityscorecard.com/

日本法人社名 ：　SecurityScorecard株式会社（セキュリティスコアカード）
本社所在地 ：　東京都千代田区丸の内一丁目 1 番 3 号
代表取締役社長 ：　藤本 大

【本件に関する連絡先】
SecurityScorecard 広報代理店 株式会社プラップジャパン
担当　菊池(070-2161-7123)、牟田(090-4845-9689)、冨安(070-2161-6963)
Email: securityscorecard@prap.co.jp