プレスリリース

報道関係各位

SecurityScorecard 株式会社

2025 年 9 月 12 日

※本抄訳リリースは、米国時間 2025 年 8 月 5 日に米国 SecurityScorecard より発表されたブログをもとに編集しています。

SecurityScorecard、イランとイスラエルの軍事衝突「12 日間戦争」における サイバー攻撃の実態を分析した調査レポートを公開

-脅威分析チーム「STRIKE」が軍事作戦と連動するサイバー攻撃の全貌を明らかに-

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」（以下、STRIKE チーム）が、**2025 年 6 月に発生したイランとイスラエルの軍事衝突「12 日間戦争」における サイバー攻撃の実態を明らかにした調査レポート（英語のみ）**を公開しました。本レポートでは、イラン革命防衛隊（以下、IRGC）と関連するハッカー集団のサイバー攻撃活動の実態を明らかにしています。

2025 年 6 月に発生したイランとイスラエルの軍事衝突「12 日間戦争」において、イランに関連するハッカーネットワークが多数のサイバー攻撃を展開していたことが判明しています。STRIKE チームは、12 日間の戦争で 178 以上のグループが発信した 25 万件のイランのプロキシからの通信を分析し、イランのハッカーやサポーター、同盟者がイランの目的を支援する形でサイバー攻撃を展開していた実態を解明しました。

主な調査結果

本調査では、攻撃キャンペーンの仕組み及び動機を考察しています。以下が主な活動内容です。

- 偵察活動の実施
- Telegram を通じた人員募集
- サイバー組織との連携
- 敵対勢力に対する制裁・諜報活動に関する議論
- 改ざんやフィッシングを用いた威嚇攻撃
- イスラエルの同盟国を標的としたマルウェア作戦
- 独自スクリプトの利用と脆弱性スキャン

- データ窃取と情報漏洩の画策
- ゼロデイやその他脆弱性の喧伝や売買

さらに、IRGC 関連グループ「Imperial Kitten」（別名：Tortoiseshell, Cuboid Sandstorm, Yellow Liderc）が軍事行動に合わせて戦術を変化させていたことも確認されています。

イランとイスラエルの「12 日間戦争」で観測されたハッカーの活動は、一見すると散発的で統一性のないものに見えましたが、分析の結果、数百に及ぶ脅威アクターの間に明確なパターンや連携の兆候が確認されています。そして、迅速かつ標的を絞った、強いイデオロギーに基づく作戦が浮き彫りになり、多くのグループが高い機動力を発揮して緊密に連携していたことが明らかになっています。

特定された脅威アクターは、下記の 3 通りに分類されます。
①IRGC（イラン革命防衛隊）に同調するが明確な任務を持たないハクティビスト
②IRGC と直接連携する集団
③国家から支援を受ける攻撃者
これらの組織的なサポーターや地域のハクティビストは、重複する標的に協調的に攻撃を仕掛けていました。しかし、規律や技術力の水準には差が見られました。

IRGC に触発された一部のグループは金融機関、政府機関、メディアを標的とし、国家と連携するグループはウェブ改ざんや業務妨害、データ窃取を展開していました。また、ハクティビストや国家から支援を受けるグループの中には「協力者」への制裁を目的とした諜報や攻撃を実施し、敵対勢力を威嚇し、イスラエルの士気低下を狙うとともに、パレスチナ支援を掲げた「サイバー戦」を拡大していました。

一部の脅威グループは IRGC の任務と密接に連動してデータ窃取や SQL インジェクション、DDoS 攻撃など展開しており、さらにイデオロギー的情熱に駆られた集団も存在することで、攻撃の帰属特定を難しくし、防御側の対応を混乱させていました。この断片的なエコシステムの中でも、Fatimion Cyber Team、Cyber Fattah、Cyber Islamic Resistance、Tunisian Maskers Cyber Force が特に注目され、防御の観点から重要な教訓を提供しています。

戦闘の激化に伴い、秘匿性の高い攻撃者も戦術を変更していました。イランと関係の深い Imperial Kitten（別名：Tortoiseshell） は、戦闘開始直後に紛争をテーマにしたフィッシング攻撃を仕掛け、即座に作戦イ

ンフラを構築しています。この攻撃キャンペーンにより、ソーシャルエンジニアリングとマルウェアを用い、脅威アクターが、紛争発生後、迅速対応可能な計画立案と任務遂行サイクルを持つことが示されました。

また、Telegram（暗号化機能や匿名性を特徴とするメッセージングアプリ）が脅威アクターの作戦手法として利用され、DDoS やウェブ改ざんといった基本的手法も依然として妨害効果を保持していることから、悪用されています。さらに、攻撃者は紛争の混乱に乗じて、攻撃のタイミングを調整し、感情操作を巧みに操り、攻撃キャンペーンを武器化していました。

本レポートでは、実際の軍事衝突下において、サイバー攻撃を防御する側にとっての重要な洞察を提示しています。空爆が国境を越えて行われる一方で、同調するサイバー攻撃者やハクティビストが、偵察、勧誘、改ざん、データ窃取、データの不正公開、フィッシング、マルウェア流布といった一連の計画的なサイバー攻撃を仕掛けています。

実際の軍事衝突と関連するハッキング攻撃が進化するのに伴い、防御もまた進化しなければなりません。大きな混乱の中でのサイバー攻撃に対抗するためには、過去の手引きに頼るだけではなく、ハッカーのやり取りや脅威をリアルタイムで監視することが求められます。

本調査レポート全文は、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

SecurityScorecard は、サプライチェーン攻撃という最も急成長している脅威に対抗するため、Supply Chain Detection and Response（SCDR）領域を立ち上げました。業界をリードするセキュリティレーティングを基盤に、サードパーティリスクを継続的にモニタリングし、要因ベースのレーティング、自動アセスメント、独自の脅威インテリジェンスを用いて脅威を防御します。また、MAX を通じてサービスパートナーと連携し、サプライチェ

ーン全体を保護し、運用におけるレジリエンス強化、第三者リスク管理の強化、単一の脆弱性からのエコシステム全体に及ぶリスクの低減を支援します。SecurityScorecard は、Fortune 100 の 3 分の 2 を含む 3,000 以上の組織に信頼され、米国サイバーセキュリティ・インフラセキュリティ庁（CISA）からも信頼できるリソースとして認められています。Evolution Equity Partners、Silver Lake Partners、Sequoia Capital、GV、NGP、Intel Capital、Riverwood Capital などを投資家に持ち、エンドツーエンドのサプライチェーンセキュリティを提供します。

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】

セキュリティスコアカード

広報代理店 株式会社プラップジャパン

担当 中田(070-7523-6980)、牟田(090-4845-9689)、冨安(070-2161-6963)

E メール:securityscorecard@prap.co.jp