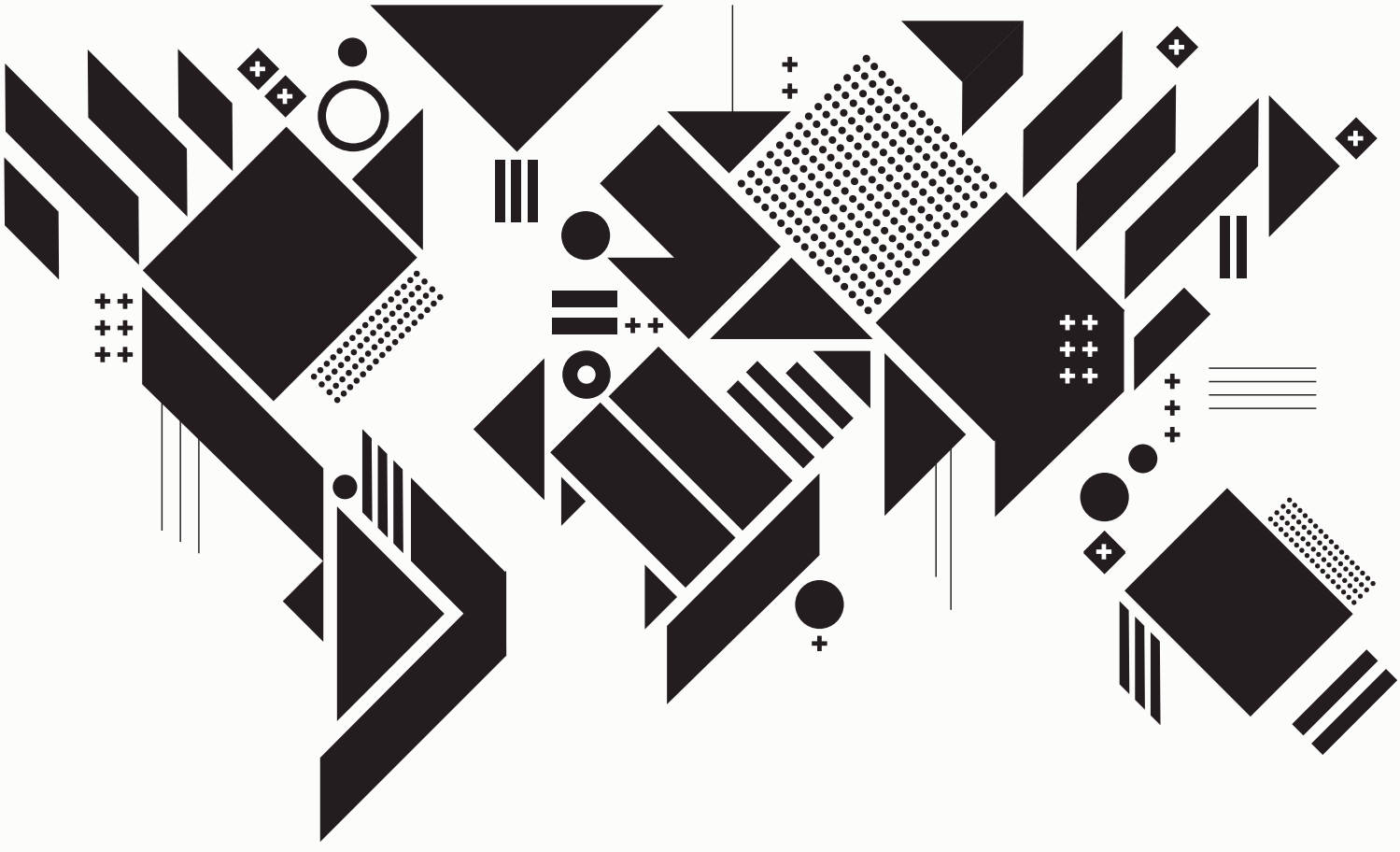
CROWDSTRIKE

2019年版
グローバル脅威レポート

攻撃者グループが身につけたノウハウと
スピードの重要性

エグゼクティブサマリー



2019年のグローバル脅威レポートでは、「CrowdStrike® Intelligence」、「Falcon OverWatch™マネージドハンティング」、および「CrowdStrike Servicesのインシデントレスポンス」の各チームが、過去1年間のサイバー脅威活動における最も重要なイベントと傾向に焦点を当てた分析結果を発表しています。この分析結果とともに提供される詳細なケーススタディは、脅威インテリジェンス、プロアクティブなハンティング、および迅速かつプロアクティブな対策が、攻撃者の動機、目的、および活動をより深く理解するためにいかに役立つかを示しています。また、重要なデータを守っていくために、その情報をどのように活用できるかについても説明しています。

2018年は、多くの点において、それまでとは大きく異なる年になりました。2017年に発生したWannaCryやNotPetyaなどのような注目を集めるイベントがなかった代わりに、2018年には、国家主導の攻撃者に対する米国司法省による一連の告発がヘッドラインを飾りました。このような発表が影響したと思われる、ツールの継続的な開発やTTP（戦術、技術、手順）の変化を見ると、2018年は多くの攻撃者にとって転換期となったようです。1つ明白なのは、法執行機関の取り組みは、まだ国家主導の攻撃を食い止めるには至っていないということです。

一つ明らかなのは、法執行機関の取り組みは、まだ国家主導の攻撃を食い止めるには至っていません。

標的を定めた侵入：止むことのない国家主導の攻撃

2018年を通じて、国家主導の攻撃者グループたちは活動を継続し、反体制派、地域の敵対勢力、さらには外国勢力を標的として、意志決定者のための情報収集を行いました。

- 北朝鮮は、外交活動を展開したのにもかかわらず、機密情報の収集と金銭取得の両方の活動を積極的に続けました。
- イランは、他の中東および北アフリカ諸国、特に湾岸協力会議（GCC）のメンバー国に対する攻撃作戦に力を入れていました。また、イランの攻撃者たちが反対勢力や少数民族を標的とした新しいモバイルマルウェアを開発していることが疑われています。
- 中国については、米国を標的とした攻撃が急増したことをCrowdStrikeが確認しています。このことはおそらく両国間の緊張が高まったことと関係していると思われます。
- ロシアの攻撃者グループらは、世界中でさまざまな情報収集や情報操作を行っていました。

サイバー犯罪者の平均９時間24分からロシアを拠点とする攻撃者の18分という驚くべき差など、攻撃者グループ間の顕著な違いを発見しました。

サイバー犯罪の経済における変化

CrowdStrike Intelligenceが調査してきたサイバー犯罪者らは、クライムウェアの配布、バンキング型トロイの木馬やランサムウェアによる攻撃、POSへの侵害、スピアフィッシング攻撃などのさまざまな犯罪活動を行ってきました。

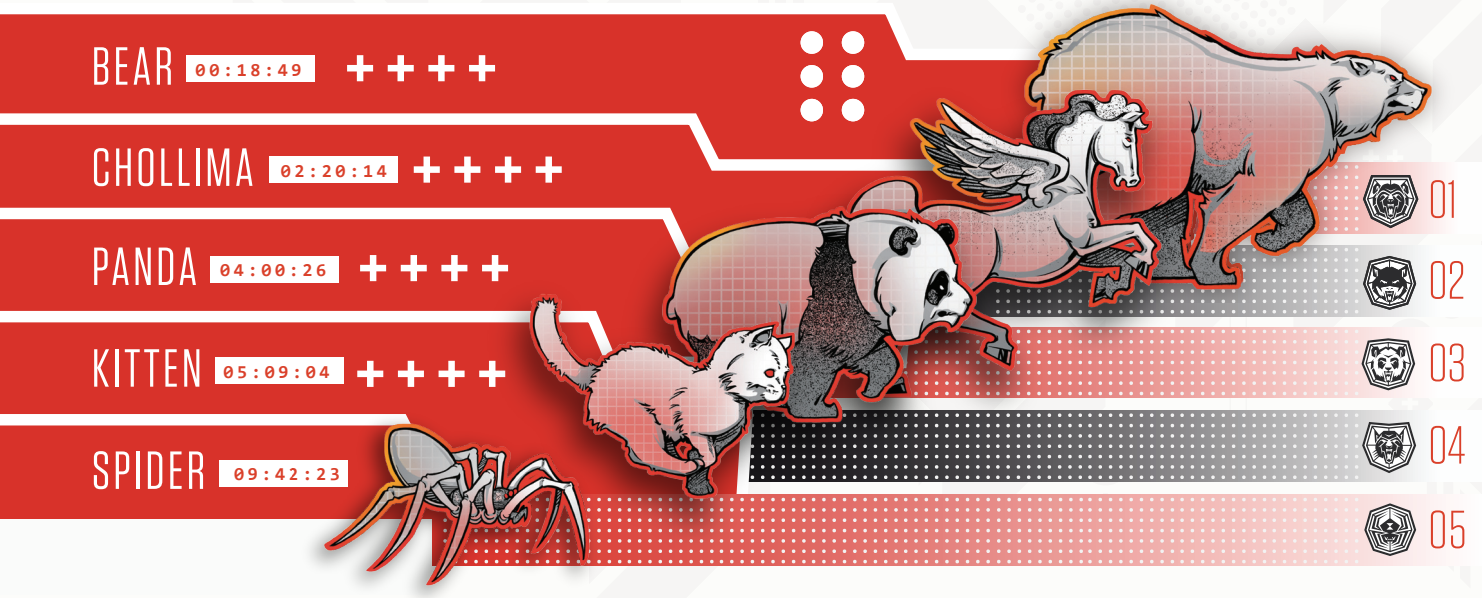
- 2018年のサイバー犯罪の最も顕著な傾向は、ターゲットを絞った侵入を試みるTTP（戦術、技術、手順）とランサムウェアを大規模な組織に展開する手法を組み合わせた「Big Game Hunting」が継続的に増加したことです。BOSS SPIDER（Samas、SamSam）、INDRIK SPIDER（Dridex）、GRIM SPIDER（Ryuk）はいずれもこのような攻撃活動を行い荒稼ぎしています。
- サイバー犯罪のエコシステムが変化していることを示すさらなる証拠としては、数多くのRaaS（ransomware-as-a-service）を使用した攻撃者グループ PINCHY SPIDER（GandCrab）、あるいは高度なマルウェア配布機能を使用するMUMMY SPIDER（Emotet）が挙げられます。
- 一方、標的型のサイバー犯罪攻撃者グループであるCOBALT SPIDER（Cobalt Group）とCARBON SPIDER（Carbanak）は、攻撃に関与した人物が逮捕されたにもかかわらず活動を続けていました。

効果的なテレメトリー：「ブレイクアウトタイム」などの重要な指標を追跡

昨年のグローバル脅威レポートでは、CrowdStrikeが追跡中の新しい重要な測定基準「ブレイクアウトタイム」に焦点を当てました。ブレイクアウトタイムとは、攻撃者が最初の侵害からどの程度の時間で被害者の環境内で水平展開に成功したかを示すものです。これは、脅威が企業環境内に蔓延して重大な被害を引き起こす前に、対処、封じ込め・修復を完了すべき制限時間を表すため、重要な指標となります。

今年、CrowdStrikeチームは、ブレイクアウトタイムをより詳しく分析し、2018年に発生した主要な攻撃者グループの侵入スピードを測定することにしました。サイバーセキュリティの世界では、攻撃と防御の両方においてスピードが物を言います。攻撃者の能力を左右するのは、ツール（購入したものであろうと、他から盗用したものであろうと）の巧妙性ではありません。それより重要なのは、攻撃者グループの攻撃活動に必要なノウハウと、標的とするネットワークで目的を達成するスピードなのです。

BREAKOUT TIME BY ADVERSARY FOR 2018



Russia:**BEAR** • North Korea:**CHOLLIMA** • China:**PANDA** • Iran:**KITTEN** • eCrime:**SPIDER**

CrowdStrikeが2018年に観測したすべての攻撃者のすべての侵入における平均のブレイクアウトタイムは4時間37分でした。しかし、この数字はすべてを語るものではありません。CrowdStrikeは、ブレイクアウトタイムの平均が9時間42分であったサイバー犯罪者グループから、ロシアを拠点とするグループのわずか18分という驚異的な記録まで、攻撃者グループ間の顕著な違いを発見しました。

攻撃者の巧妙さの判断基準はもちろんそれだけではありませんが、ブレイクアウトタイムのランキングは、彼らのオペレーション能力を評価するにはおもしろい方法です。そしてまたこのランキングは、検知・調査・対処までの平均時間（総称して「1-10-60ルール」と呼ぶ）を基準としたスピードを評価したいと考える企業の防御対策にも役立ちます。（これらの重要な防御関連の指標については、同レポートの「グローバル脅威の予測と推奨事項」のセクションでさらに詳しく説明しています。）企業は、業種や注力する地域などを鑑みつつ、最も遭遇しそうな攻撃者グループのタイプを考慮して、目標とする対応時間を検討することができるようになります。

レポート全文のダウンロード

2019年版CrowdStrikeグローバル脅威レポートでは、過去1年間におけるサイバー脅威活動の最も重要なイベントと傾向に焦点を当てた、えり抜きの分析結果を掲載しています。セキュリティの状況に関するこの重要なレポートは、http://crowdstrike.com/gtr から無料でダウンロードできます。

CrowdStrike Japan 株式会社
〒100-0005　東京都千代田区丸の内1丁目6-5
japan.sales@crowdstrike.com | crowdstrike.com/sites/jp