最新セキュリティマネジメント（第20回）

J-CRATの活動報告から学ぶ国家支援型サイバー攻撃

2023.01.24

2022年12月28日に独立行政法人情報処理推進機構はサイバーレスキュー隊の2022年度上半期の活動状況を発表した。J-CRAT（Cyber Rescure and Advice Team against targeted attack of Japan）といわれるサイバーレスキュー隊は、サイバー攻撃を受けている組織や業界、社会などを防御する使命を負っている。サイバー攻撃の最前線では何が起きているのだろうか。J-CRATの活動報告書からお伝えする。

増え続ける国家支援型と見られる攻撃

ロシアによるウクライナ侵攻や中国の台湾有事の可能性など、国際情勢が不安定さを増している中、サイバー攻撃の中身も大きく変化している。実際にウクライナ侵攻では戦車やミサイルなどによるリアルな攻撃だけでなく、システムの物理的な破壊を伴うサイバー攻撃が頻繁に行われている。

こうした中でJ-CRATの活動は、「国家支援型」とされる攻撃者によるサイバー活動の領域にも拡大している。電子的な手法を用いて政府機関や企業の情報を盗み出す「サイバーエスピオナージ」と呼ばれる活動に対して、相談対応、レスキュー活動、脅威情報の収集、悪意を持ったプログラムであるマルウエアの検知や駆除に取り組んでいる。

公開情報によると、国家支援型の標的型サイバー攻撃活動は外国の軍隊や情報機関、宣伝機関が直接手を下すだけでなく、下請けとなるハッカー集団や「政府放任型」といわれるサイバー犯罪グループを介して行われているとされる。

2022年12月に公表されたJ-CRATの2022年度上半期の活動報告によると、J-CRATが設けている「標的型サイバー攻撃特別相談窓口」に寄せられた相談・情報提供は205件。このうち緊急性が高くリモートで対応を支援する「リモートレスキュー支援」に移行したのが91件、その中でもオンサイト支援を行った事案数は15件だった。

2021年度上半期はそれぞれ128件、38件、3件という件数から考えると、標的型サイバー攻撃はますます活発になっている。近年、J-CRATでは実際の事案発生に対するレスキュー対応だけでなく、事案発生前の体制強化や事案発生後の対処についての助言活動や、マルウエアの検知や駆除といったアクティブなサイバーレスキュー活動も増えているという。

エネルギー関連分野が攻撃対象に

これまで国家支援型とされる標的型攻撃の対象となってきたのは、国内の資源・エネルギー部門に関係する組織や研究者、メディア関係者などで、2022年度上半期からは学術機関のエネルギー政策関係者を中心に、公共、金融、経済、安全保障といった分野に対する攻撃も新たに確認されている。J-CRATではこれらの攻撃を「オペレーション・エネリン」と名付けて注視している。

攻撃の手口としては滑らかな日本語の文面で、メールに記載されたリンク先から攻撃ファイルをダウンロードさせるというものだが、最近では実在する組織や関係者を詐称して、特定の受信者に対してイベントや交流会への参加依頼、取材や講演

依頼などを行い、その後のやりとりの中で攻撃ファイルをダウンロードさせる攻撃も観測されているという。

日本を取り巻くサイバー攻撃のグループはいくつかに分類される。中国に関係するサイバー攻撃グループ、ロシアに関係するサイバー攻撃グループ、北朝鮮に関係するサイバー攻撃グループがあり、その他にもイラン、インド、パキスタン、中南米、トルコなどが関与する攻撃グループがあるとされる。

中国の関与が疑われる攻撃では、日本の組織の子会社や取引先などサプライチェーンを経由して、標的となる組織に侵入して継続的な攻撃を行っていたという。多くの組織が関係する事案だけに、J-CRATでは関係すると思われる情報の提供を広く求めている。

ロシアによる攻撃の多くはウクライナ侵攻に関するもので、ウクライナのゼレンスキー大統領がロシアに降伏を表明するフェイク動画など、ウクライナ国民の士気低下や同盟諸国との分断を意図した偽装工作が行われている。日本を含む42カ国128組織に対するネットワーク侵入とスパイ活動も報告されている。

北朝鮮に関する攻撃に対しては2022年10月14日に金融庁、警察庁、内閣サイバーセキュリティセンターの連名で注意喚起が行われた。フィッシングメールやマルウエアを使って暗号資産を窃取しようという攻撃が続いているようだ。

J-CRATとしては、国家レベルでのサイバー領域での状況把握を高めながら、各組織に安全性の確認とリスクの判断、脆弱性情報などを活用した適切な対処を求めている。一般企業であっても「国家支援型」のサイバー攻撃に対するアンテナを高く張り巡らせておくべきだろう。