インバウンドコラム

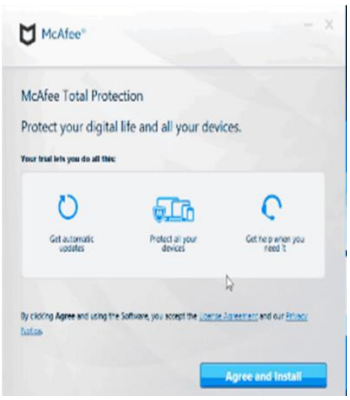
オンライン脅威への Google の取り組み

大統領選挙目前　最新の手口とは

アメリカ大統領選挙やパンデミックといった、大きなイベントの際には、サイバー攻撃の脅威が高まります。Google の脅威分析グループ(TAG：ThreatAnalysisGroup)は、当社の製品とユーザーをサイバー攻撃から保護するため、日々取り組んでいます。

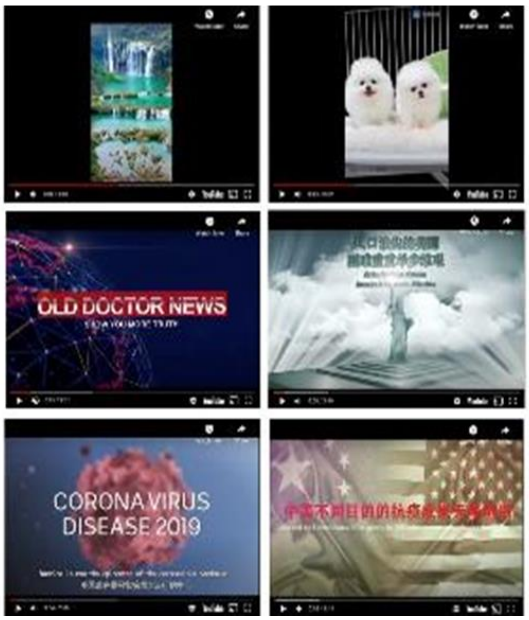
6 月、中国とイランのハッカー集団が、それぞれバイデン氏とトランプ氏両陣営へフィッシング攻撃をしかけれたことを発表しました。しかし、攻撃が成功したという証拠は見られませんでした。中国の APT31 の手口は、マカフィーになりすまし、ターゲットへ、GitHub から正規バージョンの McAfee アンチウイルスソフトウェアをインストールするよう求めるリンクをメールを送信します。リンク先のソフトウェアをインストールすると同時にマルウェアもこっそりインストールされ、攻撃者がファイルをアップロード・ダウンロードしたり、任意のコマンドを実行できるようになるというわけです。(参照※1、図 1)

図1



2019 年の夏以来、TAG は主に YouTube で活動している、中国のスパムネットワークを追跡してきました。このネットワークは様々なプラットフォームでアカウントを取得または乗っ取り、動物やゲーム、ニュース動画などのスパムコンテンツを北京語で投稿します。香港と中国の新型コロナウィルスへの対応や、米国の BLM 運動や山火事などのコンテンツを英語と北京語で投稿しています。第 3 四半期だけでも、このネットワーク関する 3,000 を超える YouTube チャンネルを削除しました。ほとんどの動画の再生回数は 10 回未満という初期段階で削除することができたため、YouTube の実際の視聴者に届いているとは考えていません。(参照※1、図 2)

図2



5 月 27 日の TAG のブログでは、2020 年 4 月に政府が支援するハッカー集団によるフィッシング攻撃の標的分布図が公表されていて、アメリカやミャンマー、マレーシア、ベトナムへの攻撃が目立ちます。(参照※2、図 3)新型コロナウィルスが収束する兆しが見えない中、今後もサイバー空間の脅威はより巧妙に進化していくと思われます。セキュリティパッチをしっかりアップデートし、怪しいメールは開かない、不用意にリンクはクリックしないよう、注意しましょう！

図3

図1～3すべて 出典元: Google Blog

※1 脅威への取り組み - Google Blog
https://blog.google/threat-analysis-group/how-were-tackling-evolving-online-threats/
※2 政府支援ハッキング対策 - Google Blog
https://blog.google/threat-analysis-group/updates-about-government-backed-hacking-and-disinformation/