Emotet感染リスクが急拡大 背景に透けるウクライナ侵攻

消滅したはずのマルウエア「Emotet」の国内感染が急拡大している。背景には、ロシアによるウクライナ侵攻の影響も見え隠れする。改正個人情報保護法の施行により、情報漏洩を起こせば新たな作業が生じる。

国内でマルウエア「Emotet(エモテット)」に感染したという事例が2022年2月から爆発的に増えている。セキュリティー企業のトレンドマイクロの調査によると、Emotetの国内検出台数は、2021年11月は524台だったが、2021年12月に検出台数が増加。2022年2月には1万8785台と急拡大した。

Emotetは遠隔操作が可能なボット型マルウエアである。攻撃者はEmotetに感染した多数のコンピューターでネットワーク(ボットネット)をつくり、一斉に操作する。Emotetに感染すれば情報が漏洩したり、スパムメール送信の踏み台にされたり、他のマルウエアに感染したりといった被害に遭う恐れがある。

ただEmotetのボットネットは1度「消滅」したはずだった。2019年から2020年に国内外で猛威を振るったEmotetに対し、欧米8カ国の法執行機関や司法当局などが協力して対抗。オランダやドイツ、ウクライナなどにあったEmotetを送信するサーバーなどを押収し、2021年1月27日に「テークダウン」を発表していた。

ここで言うテークダウンとは、サイバー犯罪者がマルウエアを遠隔操作するために設けた「C&Cサーバー」を停止させることを指す。加えて、パソコンなどに入り込んだEmotetの接続先サーバーを、C&Cサーバーから当局が用意したサーバーに変更し、Emotetを無害化するよう自動更新する取り組みも行われた。

だが、2021年11月中旬、トレンドマイクロなどの各セキュリティー組織がEmotetの活動再開を確認した。2021年1月にウクライナ警察がEmotetのC&Cサーバーの管理者を2人逮捕した。だが、「逮捕された人物は(Emotetに関する活動の)中心人物ではないともいわれ、Emotetを作成するツールを使える人物は捕まっていない可能性が高い」。トレンドマイクロの岡本勝之セキュリティエバンジェリストはこうみる。

ウィザードスパイダーが関与か

Emotetの活動再開の裏には、別のランサムウエアグループの動きが関わっている。「ウィザードスパイダーがEmotetを再構築する工作をしたことが分かっている」と米サイバー対策企業のクラウドストライクのアダム・マイヤーズ・インテリジェンス担当シニアバイスプレジデントは語る。

ウィザードスパイダーとは、ロシアやウクライナに拠点を置き、ネットバンキングの認証情報を盗んだりボットネットを構成したりするマルウエア「Trickbot(トリックボット)」を開発しているサイバー犯罪グループを指す、同社独自の呼び名だ。Emotetのボットネットを中心的に開発・運営しているとされるサイバー犯罪集団マミースパイダーとウィザードスパイダーが連携し、Trickbotのインフラを利用してEmotetをばらまいたことでEmotetが復活したとみられる。

増加するサイバー攻撃の背景には、ロシアによるウクライナ侵攻の影響も見え隠れする。ウィザードスパイダーは、Conti(コンティ)というランサムウエアを開発していることから「Conti」とも呼ばれる。Contiは、ロシアがウクライナに侵攻した後の2022年2月25日、ロシア政府に対する全面支持を表明した。

クラウドストライクのマイヤーズ氏は「他にも2つのサイバー犯罪グルー

プがウクライナに対するDDoS(分散型のサービス妨害)攻撃を仕掛けていることも確認している」と明かす。反ロシアを掲げる犯罪集団をサイバー犯罪のプラットフォームから締め出す動きもあるという。

一部のサイバー犯罪集団でナショナリズムが高まる一方で、お金もうけが目的だとはっきり宣言しているロシア系のサイバー犯罪集団もある。ただし「ロシアに対する経済制裁が続くことで、お金を稼ぐことが目的のサイバー犯罪も増えるだろう」とマイヤーズ氏は警鐘を鳴らす。

「活動を再開したEmotetによる感染被害はグローバルでも広がっているが、特に日本でその脅威が高まっている。なぜなら過去数年間、Emotetは日本をターゲットに日本語でのキャンペーンを継続的に実施してきたからだ」(マイヤーズ氏)。

マミースパイダーは組織化された犯罪集団であり、「アフィリエイト(サイバー攻撃の実行犯)に日本語ができる人が加わっていることも考えられる」(同)。日本を対象とした攻撃は進化しているというわけだ。

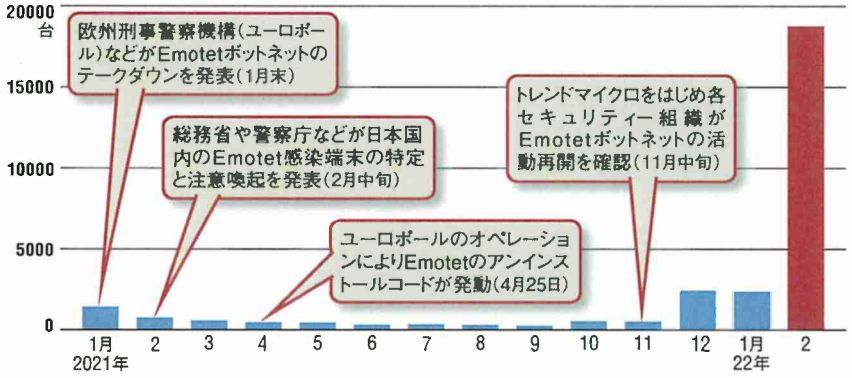
本人への通知が義務化

クラウドストライクのマイヤーズ氏は「首謀者全員が捕まらない限り、Emotetが消滅することはないだろう」と話す。企業はEmotetなどマルウエア感染の対策に一層の強化が欠かせないが、2022年4月1日からは対策を考えるうえでの留意点が1つ増えた。

それは同日に施行された改正個人情報保護法に関係するものだ。改正法は、個人情報を取り扱う事業者に対し、サイバー攻撃などの不正アクセスによって個人データの漏洩やその恐れが生じた場合、個人情報保護委員会に概要や件数、原因、再発防止策などを報告するよう義務付けた。

2022年2月に感染台数が急増

図トレンドマイクロ調査によるEmotetの国内検出台数



さらに、漏洩した個人情報について、本人にその旨を通知する義務も新たに追加した。八雲法律事務所の山岡裕明弁護士は「自社端末がEmotetに感染していると判明した時点で、被害企業には個人情報保護法に基づいた報告や通知の義務が生じる可能性が高い」と話す。

山岡弁護士は「自社が原因で取引先企業をEmotetに感染させてしまった場合、自社に過失が認められる場合には損害賠償責任を負う可能性がある点に留意する必要がある」とも指摘する。損害とは具体的に、感染経路や被害範囲を特定するために実施するデジタルフォレンジックの費用が想定されるという。ただし「感染した企業に感染対策に一定の落ち度があったと認められる場合には、感染させた企業の責任は限定される可能性があるだろう」(山岡弁護士)。

本人に対する通知義務も企業にとって負担だ。メールアドレスが分からない場合、書面を郵送する必要があるためだ。「漏洩したときのリスクも考えて、保有が必要な個人情報の項目を改めて見直す必要がある」と森・浜田松本法律事務所の蔦大輔弁護士は言う。

PPAPが感染を助長

一般に「PPAP」と呼ばれる、パスワード付きのZIPファイルをメールに添付して解凍パスワードをメールで追送するファイル共有手法は、Emotetなどのマルウエア感染を助長している側面がある。そのためPPAPでファイル共有させないようにする仕組みを導入する企業や組織が増えている。

文部科学省は2022年1月4日から、送受信メールの添付ファイルを米ボックスのクラウドストレージ「Box」に自動で移し、受信者が添付ファイルをクラウドストレージからダウンロードする仕組みを導入した。2022年3月1日、日本郵政もPPAP対策としてBoxを活用すると発表した。Box Japanによれば、同社への問い合わせ件数は2021年11月のEmotet活動再開から増え、2022年3月に急増したという。

Emotet復活やランサムウエア攻撃の増加、ウクライナ情勢などを踏まえ、日本政府は2022年2～3月、立て続けにサイバーセキュリティー対策の強化に関する注意を企業に喚起した。2月23日、3月1日に続いて3月24日にも経済産業省や総務省などが連名で注意喚起の文書を出した。

増大するサイバー攻撃リスクに対して企業は自社のセキュリティー対策を再確認することが求められる。改正個人情報保護法で加わった新たな義務を考慮に入れつつ、サイバー攻撃を受けた場合のサイバーBCP(事業継続計画)の策定など、事後対策を講じることも必要だ。 (外薗 祐理子)