サイバーレスキュー隊（J-CRAT） 活動状況
[2016 年度上半期]

2016 年 10 月 28 日
IPA（独立行政法人情報処理推進機構）
技術本部セキュリティセンター

サイバーレスキュー隊（J-CRAT）[1]における、2016 年度上半期(2016 年 4 月～2016 年 9 月)の活動状況を以下に示す。

1 活動結果

2016 年 4 月～2016 年 9 月に、「標的型サイバー攻撃特別相談窓口」に対して寄せられた相談件数と、緊急を要する事案に対してレスキュー支援を行った件数、そのうち当該組織での対応が必要と判断し隊員を派遣したオンサイト支援の件数を、表1に示す。

表 1 J-CRAT 支援件数の推移

項番	項目	2015年 上期	2015年 下期	2015年 合計	2016年 上期	2016年 下期	2016年 合計
1	相談件数	246 件	291 件	**537 件**	269 件	—	—
2	レスキュー支援数	104 件	56 件	**160 件**	68 件	—	—
3	オンサイト支援数	31 件	8 件	**39 件**	12 件	—	—

※1 1 つの事案に対して複数回のオンサイト対応を要した場合も、1件として集計

「標的型サイバー攻撃特別相談窓口」に対して寄せられた**相談件数**は **269 件**であった。このうち、**レスキュー支援**へ移行したものは **68 件**、**オンサイト支援**を行った事案数は **12 件**であった。

レスキュー支援へ移行した 68 件の組織ごとの内訳は、独立行政法人 6 件、社団・財団法人 19 件、企業 27 件、大学 6 件、地方自治体 3 件、その他・公共機関等 7 件であった。

2016 年度上半期の支援件数を、公的機関の情報漏えい事案のあった**昨年の同時期（2015 年 4 月～2015 年 9 月）**と比較すると、**相談件数**がおよそ **1.1 倍**、**レスキュー支援件数**がおよそ **0.7 倍**、**オンサイト支援件数**が **0.4 倍**となった。

2 2016 年度上半期の活動を通じてみられた特徴的な事項

(1) 標的型攻撃メールの特徴を併せ持つ日本語ばらまき型メール

6 月上旬以降、『実在する宅配便サービスや銀行からの通知を装った不審メールを受信した。標的型攻撃ではないか。』といった相談を複数受付けた。調査、分析の結果、これらは広く出回っている「ばらまき型」の不審メールであり、銀行の ID やパスワードなどを盗み取るマルウェアやランサムウェアが添付されたものであった。

銀行や宅配便サービスを題材としたばらまき型メールは昨年度より引き続き観測されているが、2016 年度上半期のばらまき型メールは、以下のような従来の標的型攻撃メールと共通する特徴を

[1] IPA が標的型サイバー攻撃の被害拡大防を目的に 2014 年 7 月に発足。相談を受けた組織の被害の低減と攻撃の連鎖の遮断を支援する活動を行っている。
https://www.ipa.go.jp/security/J-CRAT/

有していたため、受信者に標的型攻撃かもしれないという疑念を抱かせたものと思われる。

・本文に実在する通知文を転用している。

・送信元アドレスに実在するドメイン名を用いている。

・自然な日本語が用いられ、より実際の通知に類似[2]している。

なお、英文など外国語による「ばらまき型」不審メールでは .js（Java スクリプト）ファイルを zip 形式で圧縮したものが多い。一方、日本語の「ばらまき型」不審メールでは、.exe（実行）ファイルを zip 形式で暗号化したものが多く、実行ファイルが添付されたメールを削除する運用ポリシーの組織では、配信前に検知されるケースも多く見られた。

(2) 社会的・一般的な行事を題材にした、情報窃取を目的とした標的型攻撃メール

5 月中旬以降、「人事異動」「同窓会」といった一般的な題材の表題と簡素な文面に、情報窃取を目的としたマルウェアが添付された不審メールが学術・開発研究機関を中心とした複数の組織で見られた。

マルウェアの正体は「ZACOM[3]」という名称で検知される遠隔管理ツール（RAT）の一種であり、当該攻撃については 2014 年頃[4]から台湾および日本を中心に観測されているものと類似性が認められた。

今年 3 月頃にも「会員の募集」「説明会」といった一般的な題材の表題に、別種の遠隔管理ツールが添付された標的型攻撃メールを複数の組織で確認していることから、こうした簡素な文面の標的型攻撃メールを複数の組織へ送りつける手口が継続して行われていると考えられる。

3 活動を通じての提言

2016 年度上半期に活動を通じて見られた標的型サイバー攻撃の対応事例を元に、以下の通り提言する。

(1) マルウェア感染を前提とした対策の必要性

昨年度から引き続き、情報窃取を目的としたマルウェアが日本語のメールに添付されるケースが見受けられていることに加え、8 月には 2 章(2)に記載した遠隔管理ツールの亜種が新たに確認されるなどマルウェアの変化が見られているため、メールフィルタやアンチウイルスソフトで完全に防御することは困難であると考えられる。

マルウェアの感染はありえることを前提とし、被害の拡大防止を目的として、従前より提唱している出口対策に加え、特に自組織のシステム構成の把握、ファイアウォールやプロキシサーバの適切な設定といった技術面の対策、不審メール受信時の対応手順、インシデント発生時の組織的な対応体制の確立などの危機管理対策を行うことが望ましい。

(2) ファイアウォールやプロキシサーバの定期的なログ調査

ファイアウォールやプロキシサーバのログを取得していたにもかかわらず、ログの調査を行っていなかったために、攻撃に気づかないまま数年が経過していたケースが複数見られた。

ファイアウォールやプロキシサーバのログには、マルウェアに感染した端末が外部の攻撃者側と通信する際の送信元アドレスや送信先アドレスの痕跡が残る可能性がある。少しでも早い段階でマルウェア感染に気が付き、被害の拡大を防ぐためには、ログの調査を定期的に行うことが望ましい。

---

[2] 精度の低い機械翻訳のような日本語のものもあった。

[3] Nflog 型と呼ばれることもある。

[4] ZACOM として検知されるマルウェアは 2013 初夏のものも確認している。J-CRAT では、引続き本マルウェアの情報提供を求めている。

定期的なログ調査においては、通常時にどのようなログが出力されるのかを把握したうえで、それとは異なるログに着目することになる。2016 年上期のケースでは、ファイアウォールのログの中に特定サイズの通信が特定の期間に繰り返し行われた記録や、通常時は使用頻度の低い端末から外部通信先への定期的な通信が行われた記録などが見つかっている。

採取できるログの種類や形式は、情報システムの構成と用いられている機器により相違があるため、ログ調査を繰り返しながら各々の組織に合わせて調査方法を確立していくことが望ましい。特に、昨今の攻撃手法では、通常通信に攻撃通信を紛れ込ませるものが主流のため、通信要件に合わない通信を記録するだけでなく、通常通信の記録もログとして取得しないと発見は極めて困難となる。

(3) DNS サーバログの適切な利活用

組織内に独自の DNS サーバを設置していた組織でマルウェア感染が見つかった際に、DNS サーバのログが取られていないケースが複数みられた。

DNS サーバのログには、マルウェアに感染した端末が外部の攻撃者側と通信する際に名前解決を行った痕跡が残る可能性がある。名前解決の記録と不正通信先のリストとを照合することで、システムの感染状況をより早く把握し、原因究明に役立てることができる。

2016 年上期のケースでは、IP アドレスが頻繁に変更される不正通信先との通信記録を調査するにあたり、DNS サーバのログが無いために調査範囲が拡大したことがあった。

DNS サーバのログを取得する際は、ファイアウォールなどその他の機器と組み合わせて調査することを念頭に、必要なログ項目、記録期間を設定することが望ましい。

特に、攻撃の過程においては、名前解決結果が 0.0.0.0 や 127.0.0.1 となり、感染端末から外部へ通信を発生させないよう潜伏することがあるため、そのような「一般にはとりえない名前解決結果を検知する」、「構成上、名前解決をする必要がない端末からの要求を記録する」など、DNS 通信自体を観測することで、感染後の調査に役立てることができる。

(4) 情報共有活動への積極的な参加

J-CRAT では、標的型攻撃に関する相談や情報提供を元に攻撃の連鎖をたどるとともに、提供された情報、抽出した攻撃の特徴を関連する組織へ提供することで被害の早期検知と拡大防止に努めている。

当隊の活動は攻撃情報を得た組織からの相談や情報提供に支えられており、日々変化する標的型攻撃を追うためには情報共有の輪を拡大することが必要不可欠であると考える。

社会全体のサイバー攻撃対応能力の向上のため、各組織は、IPA や JPCERT コーディネーションセンターや警察、関連団体等からの注意喚起情報を自組織のサイバーセキュリティ対策に活かすとともに、インシデント発生時、そしてインシデント発生後の情報共有に、積極的に参加[5]することをお願いしたい。

[5] サイバーセキュリティ経営ガイドライン Ver 1.0
(8)情報共有活動への参加を通じた攻撃情報の入手とその有効活用のための環境整備
http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf

企業経営のためのサイバーセキュリティの考え方の策定について
2－③ サプライチェーン全体でのサイバーセキュリティの確保
http://www.nisc.go.jp/active/kihon/pdf/keiei.pdf