サイバーセキュリティレポート

2022.11

NTT セキュリティ・ジャパン株式会社
コンサルティングサービス部　OSINT モニタリングチーム

目次

1. 大阪急性期・総合医療センターにランサムウェア攻撃、電子カルテシステムに障害 3
1.1. 概要 3
1.2. 事件の経緯 3
1.3. 攻撃者と侵入経路 4
1.4. 政府の対応 6
1.5. まとめ 6
2. 再始動した EMOTET 7
2.1. 概要 7
2.2. これまでの EMOTET 7
2.3. Microsoft 社の対策と EMOTET 側の対策 8
2.4. まとめ 10
3. フィッシング攻撃を容易にするサービス「Robin Banks」 11
3.1. 概要 11
3.2. PhaaS 11
3.3. Robin Banks 12
3.4. Robin Banks のサービス再開 14
3.5. まとめ 15

【当レポートについて】

当レポートでは 2022 年 11 月中に生じた様々な情報セキュリティに関する事件、事象、またそれらを取り巻く環境の変化の中から特に重要と考えられるトピック 3 点を選び、まとめたものである。各トピックの要旨は以下のとおりである。

第 1 章『大阪急性期・総合医療センターにランサムウェア攻撃、電子カルテシステムに障害』

- 11 月 1 日、内閣官房長官は大阪急性期・総合医療センターが受けたランサムウェア攻撃について、専門家を現地に派遣し対応を行っていることを記者会見で明らかにした。
- 給食を納入していた業者のシステム経由での侵入が疑われている。この業者は VPN 装置をアップデートせずに利用していた。
- 医療センター側は、ファームウェアやセキュリティソフトのアップデート等の対策を行っていたが、給食業者経由での侵入は想定していなかったと述べている。本件はサプライチェーン全体での対策の難しさと重要さを示す事例であると考えられる。

第 2 章『再始動した EMOTET』

- 2022 年 7 月から休止していた EMOTET マルウェアの感染拡大を狙うメールの送信活動が、11 月に入り再始動した。
- EMOTET マルウェアは主に、メール添付の Office マクロファイルの実行を介して端末に感染する。Microsoft 社は対策として 7 月にメールから Office マクロファイルを実行できないよう Office の実装を変更したが、今回の再始動ではその対策を回避するようユーザーに指示することで感染を狙っており、攻撃者の工夫がみられる。
- 今回は大きな被害は無い模様で工夫は効果的でなかったとみられ、今後、これまで使用したことがある他の感染手法や新しく開発した手法で EMOTET 感染を狙う可能性が考えられる。

第 3 章『フィッシング攻撃を容易にするサービス「Robin Banks」』

- PhaaS とは、フィッシングに必要なツールや運用（ホスティングを含むフィッシングサイトの構築、フィッシングメールの送信等）を、サブスクリプション形式で提供するサービスである 。
- PhaaS の一つ「Robin Banks」は、金融機関等に偽装したフィッシングを簡単に実行できるようサービスを提供している。6 月に大規模なフィッシングキャンペーンに使用された後ネットワークを止められたが、11 月になり、多要素認証の回避等の機能を強化してサービスを再開させた。
- Robin Banks は、攻撃できるターゲットを個人の金融情報から組織のクラウドの認証へと広げようとしていると考えられる。組織は FIDO 認証を導入するなど、フィッシング攻撃への対策を講じることがこれまで以上に求められている。

1. 大阪急性期・総合医療センターにランサムウェア攻撃、電子カルテシステムに障害

1.1. 概要

2022 年 11 月 1 日、松野博一内閣官房長官は、大阪の高度救命救急センターに指定されている「大阪急性期・総合医療センター」(以降、「医療センター」もしくは「同センター」と呼ぶ)がランサムウェアによるサイバー攻撃を受けたことから、専門家を現地に派遣し対応を行っていることを記者会見で明らかにした[1]。この攻撃によって、同センターの電子カルテシステムは利用できなくなり、サーバーには身代金を要求するメッセージが表示されていた。同センターは外来診療や緊急時以外の手術を停止することになった。

図 1 大阪急性期・総合医療センター[2]

1.2. 事件の経緯

【事件発覚】

10 月 31 日午前 6 時頃、医療センターに給食を提供していた事業者のシステムで障害が発生。続いて病院の電子カルテシステムにも障害がみられた。同センターの職員から連絡を受けたシステム事業者がサーバーを確認したところ、「すべてのファイルを暗号化した。復元したければビットコインで支払え。我々にどれだけ早く連絡するかによって、金額は変わる。」という内容の英文メッセージが表示されていた[3]。実際にファイルは暗号化されており、システムが利用できない状態であった。同センターは午後 8 時頃から記者会見を開き、ランサムウェア攻撃を受けた可能性が高いと発表した。

[1] 出典：REUTERS『医療センターへのサイバー攻撃、復旧めど立たず 専門家派遣＝官房長官』
https://jp.reuters.com/article/jp-osaka-cyber-idJPKBN2RR2FD

[2] 出典：大阪府急性期・総合医療センター『理念・基本方針』
https://www.gh.opho.jp/hospital/2.html

[3] 出典：NHK『大阪急性期・総合医療センターでシステム障害 サイバー攻撃か』
https://www3.nhk.or.jp/news/html/20221031/k10013876181000.html

【被害状況】

医療センターには 36 の診療科があり、急性期から回復期まで、あらゆる疾患に対する医療を提供している[4]。また、高度救命救急センターとしては 24 時間体制を敷いている。更に大災害に対応する基幹災害医療センターにも、大阪府で唯一指定されている[5]。

今回の攻撃で医療センターの約 2,300 台の機器のうち、バックアップを含む基幹サーバー、電子カルテシステム関連のサーバー、パソコン等約 1,300 台において、ファイルが暗号化される等の影響を受けた[6]。その結果、緊急時以外の手術や外来診療を停止することになった。また、薬の処方システムにも影響が及んだことから、既存の患者については紙のカルテで対応を行うことになった[7]。発生当日の 10 月 31 日だけでおよそ 1,000 人の患者に影響があったが、患者の健康状態にかかわる問題はなかった[8]。

【復旧作業】

バックアップを保存していた基幹系サーバーも被害にあったが[6]、事件発生 4 日前の 10 月 27 日午後 9 時時点のバックアップが磁気テープで保存されており、そのデータを元に現在も復旧作業が行われている[9]。

11 月 10 日には、部分的ではあるが電子カルテの参照が可能な環境が用意され、利用できるようになった。12 月 12 日に病院関係者は、電子カルテを含む多くの機能が使えるようになったが、未だ完全な復旧には至っていないと述べている[10]。同センターは今後、基幹システムを再構築し、バックアップからの復旧作業やテストを行う予定であり、来年 1 月下旬の完全復旧を目指している[9]。

1.3. 攻撃者と侵入経路

【侵入経路】

11 月 7 日、医療センターは記者会見を行い、政府の派遣した専門家チームによる調査状況等を発表した[11]。それによると、攻撃者は先に給食事業者である「ベルキッチン」に攻撃を行い、そのデータセンター経由で医療センターのシステムへ侵入し

---

[4] 出典：大阪急性期・総合医療センター『知ってる?大阪府立病院のミッション』
https://www.opho.jp/mission/kyuseiki/

[5] 出典：大阪急性期・総合医療センター『総長あいさつ』
https://www.gh.opho.jp/hospital/29.html

[6] 出典：産経新聞『＜特報＞侵入の〝突破口〟は給食提供業者か、大阪・病院サイバー攻撃１週間　完全復旧は年越しへ』
https://www.sankei.com/article/20221107-XL4VCY2DCNJATA7Y4LJL26EZNU/

[7] 出典：NHK NEWS WEB『大阪急性期・総合医療センター サイバー攻撃で診療影響続く』
https://www3.nhk.or.jp/kansai-news/20221101/2000067859.html

[8] 出典：朝日新聞 DIGITAL『大阪の医療センターにサイバー攻撃　手術延期、外来診療できない状態』
https://www.asahi.com/articles/ASQB075DWQB0OXIE022.html

[9] 出典：日経 XTECH『ランサムウエア被害の大阪急性期・総合医療センター、感染経路と復旧工程が明らかに』
https://xtech.nikkei.com/atcl/nxt/column/18/00001/07348/

[10] 出典：日経新聞『サイバー攻撃受けた大阪の病院、電子カルテの機能復旧』
https://www.nikkei.com/article/DGXZQOUF128X50S2A211C2000000/

[11] 出典：ITmedia『大阪・病院サイバー攻撃の侵入口業者、徳島の被害病院と同一の VPN 利用』
https://www.itmedia.co.jp/news/articles/2211/08/news073.html

たと考えられている[6]。

ベルキッチンのシステムで利用されていた VPN 装置は、昨年**ランサムウェア攻撃を受けた半田病院が利用していたものと同一であり、2020 年以降一度もアップデートされておらず、脆弱性が含まれたままであった**[12,13]。ベルキッチンと医療センターの両システム間は、ベルキッチン側の仕様で、**リモートデスクトップで常時接続されていた** [13,14]。犯人はベルキッチンの VPN 装置を攻撃した後、医療センターとのリモートデスクトップ接続を利用し、侵入したと見られている。

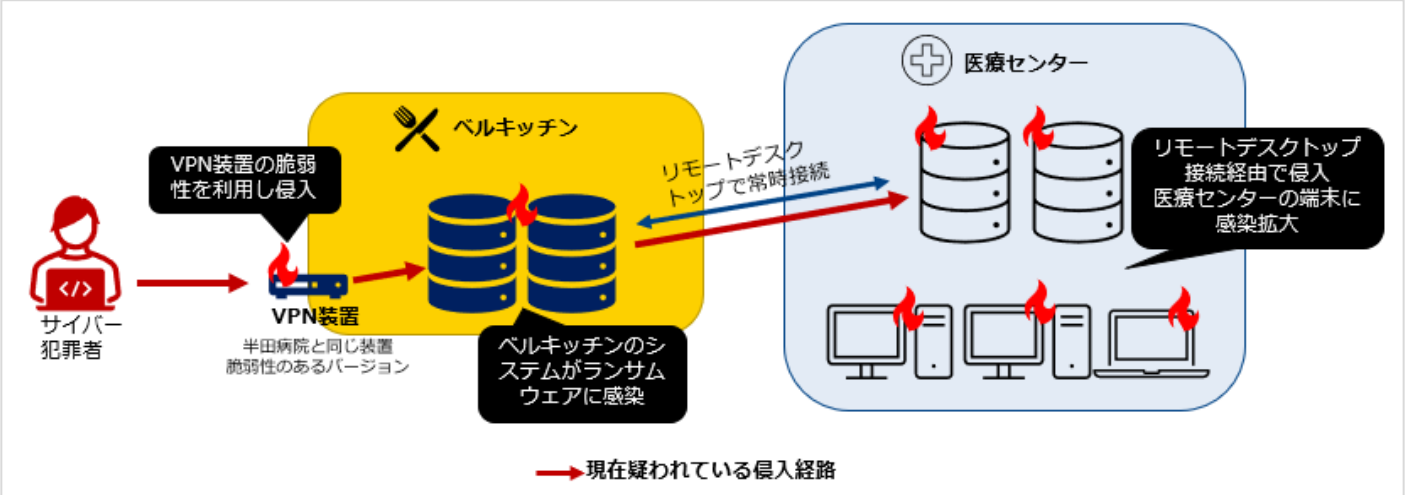

図 2 感染フロー概略図

図 3 ベルキッチンで利用されていた VPN 装置
(メーカー側の分類上は「次世代ファイアウォール」)[15]

医療センター側は、セキュリティ機器のファームウェアやサーバーのウイルス対策ソフトのアップデートを毎週行うといった対策を実施していたが、攻撃者が侵入後にウイルス対策の機能を停止した形跡があった。

---

[12] 出典：大阪・病院サイバー攻撃の侵入口業者、徳島の被害病院と同一の VPN 利用
https://www.itmedia.co.jp/news/articles/2211/08/news073.html

[13] 出典：読売新聞オンライン『大阪・病院サイバー被害　侵入口の接続記録消え、攻撃元特定困難に…政府チーム調査』
https://www.yomiuri.co.jp/local/kansai/news/20221122-OYO1T50006/

[14] 出典：Yahoo!ニュース(MBSNEWS)『【速報】大阪・堺市の「給食提供施設」にもサイバー攻撃　31 日に攻撃があった『大阪急性期・総合医療センター』に給食提供　吉村知事「給食事業者のサーバーから侵入した可能性高い」業者の機器は去年サイバー攻撃受けた徳島の病院と同一』
https://news.yahoo.co.jp/articles/43e822ce854ca57a806911d2351595d5cf77a9d8

[15] 出典：Fortinet『FortiGate 60E シリーズ』
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/ja_jp/FGT60EDS.pdf

【攻撃者】

この事件はランサムウェアグループ「Phobos(フォボス)」の犯行とみられている[16]。同グループは医療業界をターゲットとすることが多く、電子メールによるフィッシングやリモートデスクトップを介したシステムへの侵入といった手口で知られている[17]。昨年、米国の保健福祉省（Department of Health and Human Services [HHS]）も同グループの分析レポートを発表し、医療関係者に注意を促している[18]。

1.4. 政府の対応

近年、増加するランサムウェア攻撃により医療機関が被害に遭うケースが増えていることから、厚生労働省は今年 3 月、「医療情報システムの安全管理に関するガイドライン」を改訂する等、対策の強化を呼び掛けている[19]。

改定版では、ランサムウェアによってサーバーやネットワーク上のストレージが攻撃を受けることも想定し、それらから切り離したバックアップも保全することや、被害にあった際に早急に対処できるよう、ネットワーク構成図やシステム構成図、システム責任者一覧等を整備しておくこと等を推奨している。

また、政府と日本医師会などが協力し医療分野のサイバー攻撃対策の情報を収集、共有する新組織が設立される予定であり、厚生労働省は年内にも専門家を交えた検討チームを設け、運営方法などを具体化する[20]。

1.5. まとめ

本件については政府から派遣された専門家を含めたチームにより復旧作業と調査が今も進められており、詳細は今後の発表を待ちたい。

注目したいのが、侵入経路である。現在までに発表されている情報によると、給食業者のシステム経由で侵入するサプライチェーン攻撃が実行された可能性が高い。医療センター側は、ファームウェアやセキュリティソフトのアップデート等の対策を行っていたが、給食業者経由での侵入は想定していなかったと述べている。自社が慎重にセキュリティ対策を施しても取引業者の対策不備によって侵入されてしまう場合があるという点で、本件はサプライチェーン全体での対策の難しさと重要さを示す事例であると考えられる。

---

[16] 出典：朝日新聞 DIGITAL『サイバー攻撃の連鎖か　大阪の病院、システム接続の別法人も被害判明』
https://www.asahi.com/articles/ASQC75HZ5QC7ULZU00N.html

[17] 出典：BlackBerry『Phobos ランサムウェアは恐るるに足らず』
https://blogs.blackberry.com/ja/jp/2021/11/threat-thursday-phobos-ransomware

[18] 出典：HHS『Overview of Phobos Ransomware』
https://www.hhs.gov/sites/default/files/overview-phobos-ransomware.pdf

[19] 出典：厚生労働省『医療情報システムの安全管理に関するガイドライン』
https://www.mhlw.go.jp/content/10808000/000936160.pdf

[20] 出典：産経新聞『政府×日医　病院サイバー対策で新組織設立へ』
https://www.sankei.com/article/20221127-VNQBMBAIMNN5TPPURWGONRUNKQ/

2. 再始動した EMOTET

2.1. 概要

EMOTET マルウェアはサイバー攻撃者グループである EMOTET グループが用いるトロイの木馬型のマルウェアであり、メール添付等を介して感染する。情報窃取の他、ランサムウェア感染に繋がるため恐れられてきた。

2022 年 7 月から EMOTET グループはメール送信活動を休止していたが、11 月に入り再始動した。メールには従来と同様にマルウェアのダウンローダーである Microsoft Office マクロファイルが添付されていた。ただし、このマクロファイルには Microsoft 社が感染防止のために 7 月に実装した、マクロ実行防止策を回避しようとする工夫が見られた。[21]

2.2. これまでの EMOTET

2019 年に観測されて以来、EMOTET グループは活動と休止を繰り返してきた。法執行機関による 2021 年 1 月の捜査でサーバーの差し押さえを受けて潜伏したものの、同年 11 月から活動を再開した。ところが 2022 年 7 月になると EMOTET グループはメールの送信を停止した。

インターネット上にあるマルウェア感染のための攻撃インフラがそのまま[22]であったため、EMOTET グループは健在ではあるもののメール送信活動は休止に入ったとセキュリティ研究者は推測した。9 月から、攻撃インフラにある EMOTET マルウェアに情報窃取機能の強化等のアップデートが相次いだため、セキュリティ研究者は再始動が近いと考えた[23]。予想通り、グループは 11 月 2 日から再びメールを送信するようになった。日本語のメールを含め、様々な言語のメールが確認されている(図 4) 。

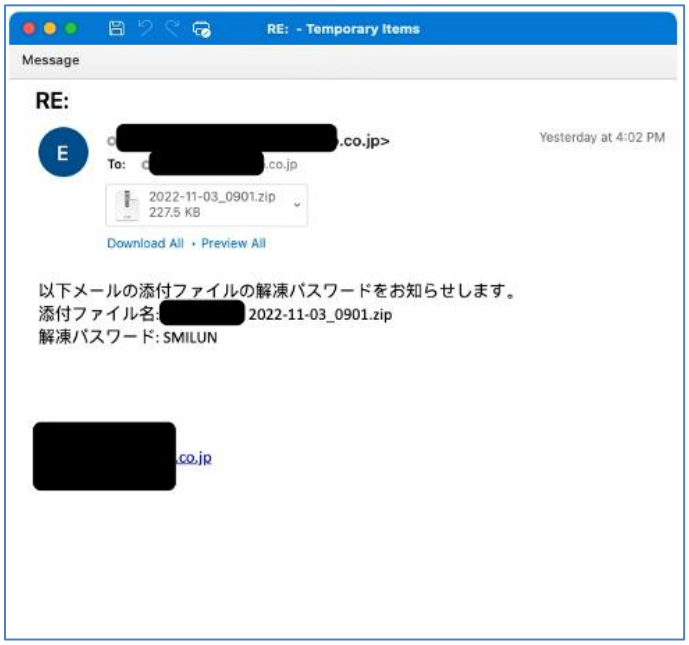

図 4 2022 年 11 月に確認された、EMOTET グループによる日本語メール [24]

[21] 出典：JPCERT/CC『マルウェア Emotet の感染再拡大に関する注意喚起』
https://www.jpcert.or.jp/at/2022/at220006.html

[22] 出典：BLEEPINGCOMPUTER『Emotet botnet now pushes Quantum and BlackCat ransomware』
https://www.bleepingcomputer.com/news/security/emotet-botnet-now-pushes-quantum-and-blackcat-ransomware/

[23] 出典：トレンドマイクロ『EMOTET のボットネットが攻撃メール送信を再開』
https://www.trendmicro.com/ja_jp/research/22/k/emotet-botnet-resumes-sending-attack-emails.html

[24] 出典：Proofpoint『2022 年秋の Emotet の復活を総合的に考える』
https://www.proofpoint.com/jp/blog/threat-insight/comprehensive-look-emotets-fall-2022-return

2.3. Microsoft 社の対策と EMOTET 側の対策

【マクロファイルを狙ってきた EMOTET グループ】

マルウェアを直接メールに添付すると、ウイルス対策ソフトで検知される等によりターゲットを感染させることが難しい。そこで EMOTET グループは Office マクロファイルを経由して感染させる仕組みを利用してきた。Office 形式のファイルはビジネスメールへの偽装とマッチしていて疑われにくいということもあり、この攻撃手法は多くの感染被害に繋がってきた。

ダウンローダーとなる Office マクロファイルには、マルウェアをインターネット上からダウンロードして感染させるマクロが組み込まれている。標準ではマクロが無効になっておりファイルを開いただけでは感染しないため、EMOTET グループはソーシャルエンジニアリングによってユーザーにマクロを有効にさせようとする。ファイルの文面にはセキュリティ警告のバーにある「コンテンツの有効化」をクリックするよう促す説明が記されていて、騙されたユーザーがクリックするとマクロが有効になり自動的にマルウェア感染する仕組みになっている（図 5）[25]。

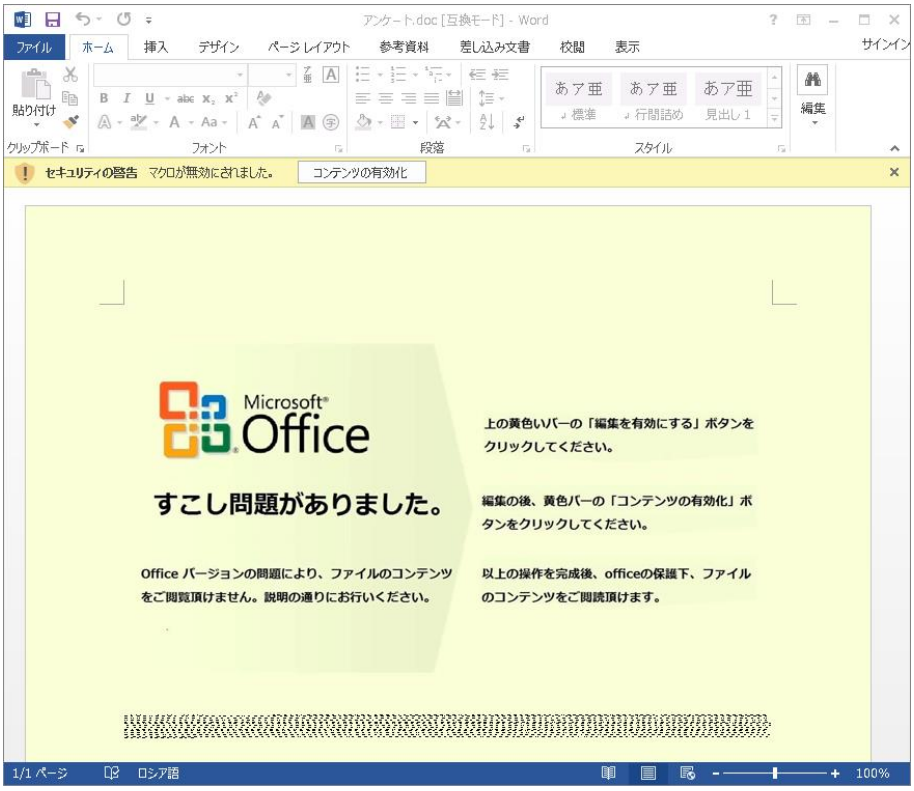

図 5 2020 年に確認された、EMOTET マルウェア感染へと誘導する Office マクロファイルの文面

【Microsoft 社のマクロファイル対策】

2022 年 7 月に Microsoft 社は、メールから開いた Office マクロファイルがセキュリティの警告バーと「コンテンツの有効化」ボタンを表示しないよう、仕様を変更した。ユーザーが誤ってマクロを実行し EMOTET マルウェア等に感染することの防止を狙

[25] 出典：JPCERT/CC『マルウエア Emotet への対応 FAQ』
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

ったものである[26]。効果はすぐに現れ、メールセキュリティの Hornetsecurity 社の観測では、メールによる攻撃のうち Excel ファイルを使用した攻撃が占める割合が対策前は 14.4 %だったのが対策直後には 5.1 %に減少[27]した。攻撃者が Excel の Office マクロファイルを使用しなくなった影響と同社は分析している。

【ソーシャルエンジニアリングを使った回避策】

11 月の再始動後の EMOTET グループは、Microsoft 社の対策を意識したソーシャルエンジニアリング攻撃を行うようになった[28]。

Office マクロファイルを送信するのは変わらないが、大きな変化として**ファイルの文面が、当該ファイルを特定の「信頼できる場所」のフォルダにコピーしてからマクロを実行するよう促す注意書きに変更された**(図 6)。マクロはメール添付のまま開いた場合は実行できないが、**「信頼できる場所」へコピーすると以前と変わらずに実行可能**となるため、Microsoft 社による対策の回避を狙ったと考えられている（図 7）。

なおこの方法はファイルのコピー操作に手間がかかることや、マクロ実行時に管理者権限の確認のウインドウが表示されて、権限の無いユーザーは実行できないため、被害に繋がる可能性は低いとセキュリティ研究者は分析している [29]。

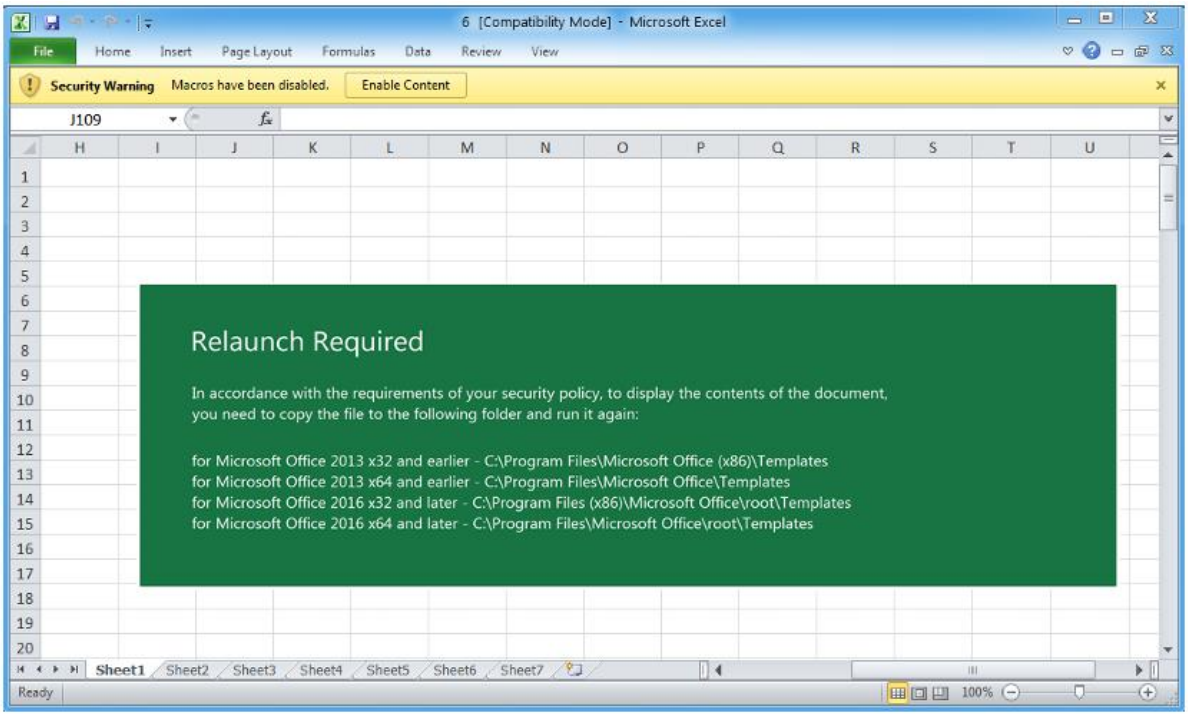

図 6「信頼できる場所」にコピーして実行することを求める Office マクロファイル [30]

[26] 出典：ログミーBiz『Microsoft が施したマクロブロックは分水嶺だった　あらためて警戒すべきマルウェア＆ランサムウェアの感染経路とその手口』
https://logmi.jp/business/articles/327627

[27] 出典：Hornetsecurity『Email Threat Review July 2022』
https://www.hornetsecurity.com/en/threat-research/email-threat-review-july-2022/

[28] 出典：JPCERT/CC『マルウェア Emotet の感染再拡大に関する注意喚起』
https://www.jpcert.or.jp/at/2022/at220006.html

[29] 出典：トレンドマイクロ『攻撃手法から考える防御策 2022 年 11 月に活動再開した EMOTET（エモテット）を既存環境で防ぐ考え方』
https://www.trendmicro.com/ja_jp/jp-security/22/k/securitytrend-20221114-01.html

[30] 出典：トレンドマイクロ『攻撃手法から考える防御策 2022 年 11 月に活動再開した EMOTET（エモテット）を既存環境で防ぐ考え方』
https://www.trendmicro.com/ja_jp/jp-security/22/k/securitytrend-20221114-01.html

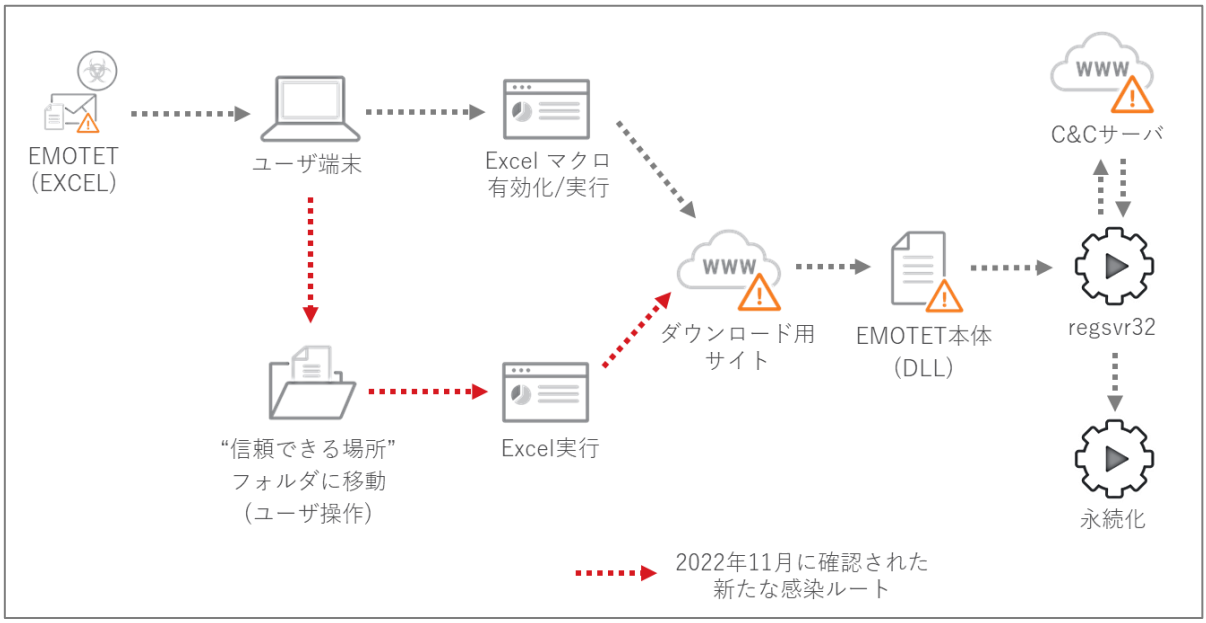

図 7 Office マクロファイルによる感染の流れ(2022 年 11 月～)

トレンドマイクロ社の記事より [31]

2.4. まとめ

再始動した EMOTET グループは、Office マクロファイルを感染手段として利用し続けようと工夫した。しかしこの工夫は効果的とは考え難い方法であり、感染被害の情報も以前ほど見られない。11 月末にはメール送信活動を低調化させた模様である[32]。

今後、EMOTET グループが Office マクロファイル方式を諦めて、ショートカットファイルの添付といったこれまで使用したことがある他の感染手法[33]や新しく開発した手法で感染拡大を図る可能性が予想される。

[31] 出典：トレンドマイクロ『攻撃手法から考える防御策 2022 年 11 月に活動再開した EMOTET（エモテット）を既存環境で防ぐ考え方』
https://www.trendmicro.com/ja_jp/jp-security/22/k/securitytrend-20221114-01.html

[32] 出典：TG Soft『News - Malware & Hoax』
https://www.tgsoft.it/news/news_archivio.asp?id=1366

[33] 出典：ログミーBiz『Microsoft が施したマクロブロックは分水嶺だった あらためて警戒すべきマルウェア＆ランサムウェアの感染経路とその手口』
https://logmi.jp/business/articles/327627

3. フィッシング攻撃を容易にするサービス「Robin Banks」

3.1. 概要

PhaaS と呼ばれる、フィッシングをサポートするサービスが、認証情報を狙ったフィッシング攻撃への参入障壁を下げている。その中でも特に Robin Banks は、 フィッシングツールのパワーアップを繰り返しており、技術レベルが低いサイバー犯罪者でも多要素認証を回避してフィッシング攻撃ができるよう、サービス機能を充実させている。

3.2. PhaaS

PhaaS（Phishing-as-a-Service [サービスとしてのフィッシング]）とは、フィッシングに必要なツールや運用（ホスティングを含むフィッシングサイトの構築、フィッシングメールの送信等）を、サブスクリプション形式で提供するサービスである[34]。クレジットカード情報や金融機関に紐づく認証情報等を狙うサイバー犯罪者に利用されており、技術レベルの低いサイバー犯罪者であっても、コストをかけずにフィッシング攻撃を実行できる。PhaaS で盗まれた認証情報は、クレジットカードの不正利用等、金銭目当ての犯罪に利用されている。また、ダークウェブ等での転売も行われている。

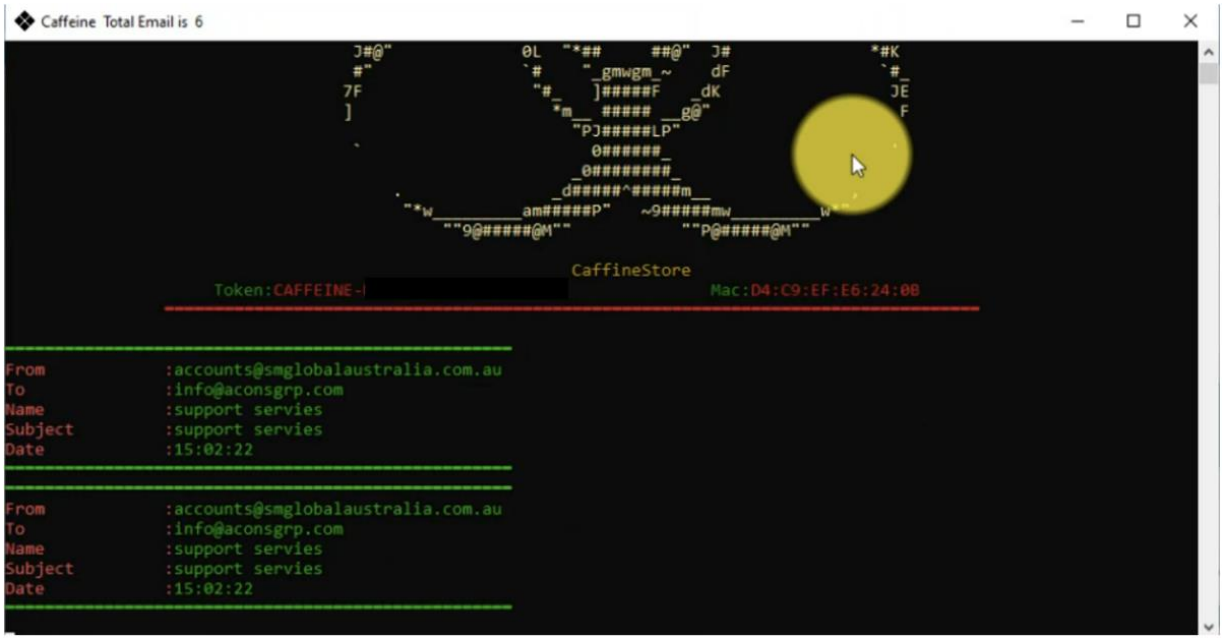

図 8 PhaaS が提供する E メール送信ツール[35]

[34] 出典：クラウド Watch『NTT データによる 2021 年のサイバーセキュリティ振り返りと 2022 年の予測 ランサムウェア被害の継続とフィッシングの as-a-Service が深刻に』
https://cloud.watch.impress.co.jp/docs/special/1377438.html

[35] 出典：Mandiant『The Fresh Phish Market: Behind the Scenes of the Caffeine Phishing-as-a-Service Platform』
https://www.mandiant.com/resources/blog/caffeine-phishing-service-platform

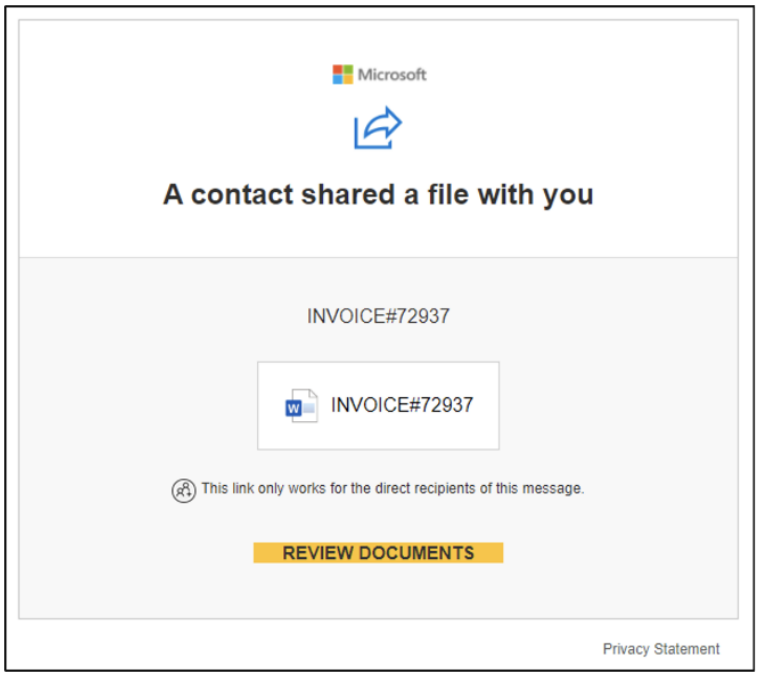

図 9 請求書を偽装するフィッシングメール用のテンプレート

3.3. Robin Banks[36]

Robin Banks と呼ばれる PhaaS が初めて確認されたのは 2022 年 3 月。同サービスは、継続的なアップデートと 24 時間年中無休のサポートを提供する月契約のサブスクリプションとなっている。契約を結ぶと、同サービスの Web サイトにログインし、新しいフィッシングサイトの作成や、管理インターフェースでのフィッシングサイトの監視を行うことができる。

図 10 Robin Banks の管理インターフェース

フィッシングを行うサイバー犯罪者は、Robin Banks を利用することで、主に米国を拠点とする金融会社（Bank of

[36] 出典：IronNet『Robin Banks might be robbing your bank』
https://www.ironnet.com/blog/robin-banks-a-new-phishing-as-a-service-platform

America、Capital One、Citibank、Wells Fargo 等）や主要クラウドサービス（Google、Microsoft 等）に偽装したフィッシング攻撃をメニューから選ぶだけで実行できる。

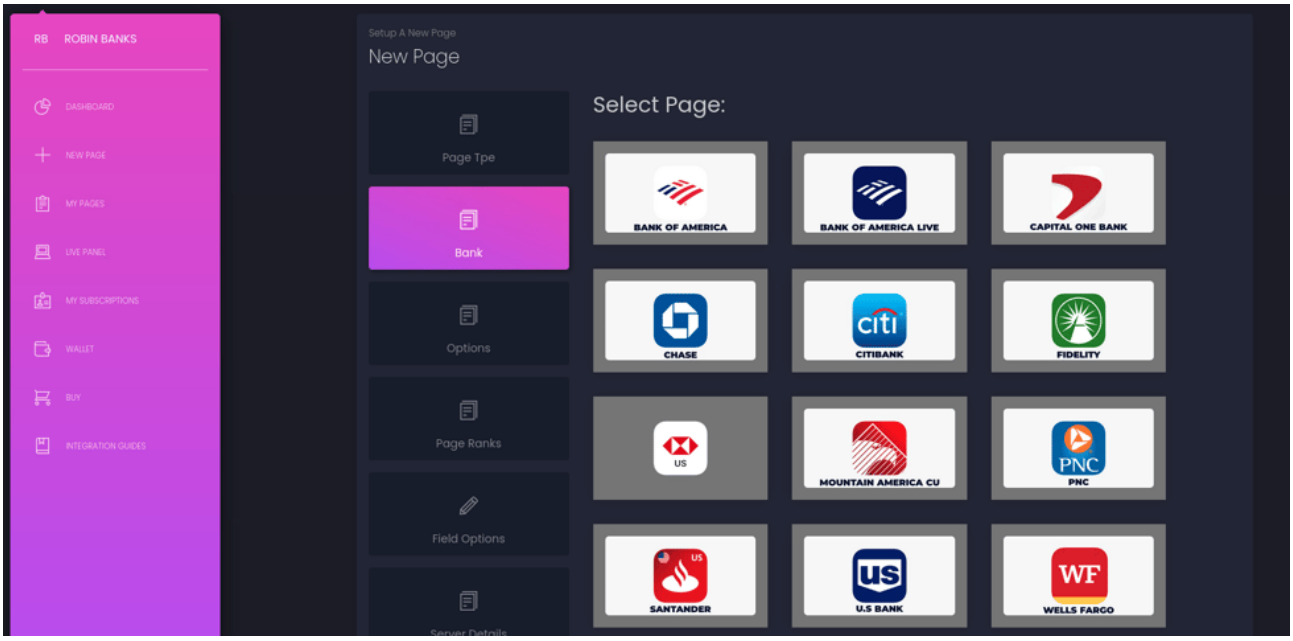

図 11 Robin Banks のフィッシングサイト作成ページ

【Robin Banks の攻撃キャンペーンと停止】

2022 年 6 月、Robin Banks を利用した大規模な攻撃キャンペーンが観測された。Microsoft や Citibank の認証情報が窃取され、その多くはダークウェブやさまざまな Telegram チャネルを介して販売された。

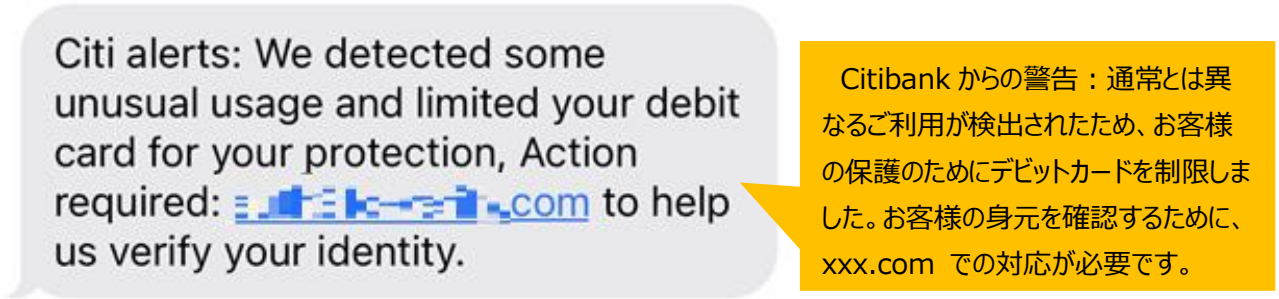

図 12 攻撃キャンペーンで使われた SMS の例 [37]

しかし、2022 年 7 月、米セキュリティ企業である IronNet 社が Robin Banks の活動についての記事をリリース。その後、ホスティングに利用されていた大手 CDN である Cloudflare が関連ドメインをブラックリストへ登録したため、サービスが停止するに至った[38]。

[37] 出典：IronNet『Robin Banks might be robbing your bank』
https://www.ironnet.com/blog/robin-banks-a-new-phishing-as-a-service-platform

[38] 出典：IronNet『Robin Banks still might be robbing your bank (part 2)』
https://www.ironnet.com/blog/robin-banks-still-might-be-robbing-your-bank-part-2

3.4. Robin Banks のサービス再開

2022 年 11 月、Robin Banks がロシアのプロバイダーである DDOS-GUARD にサーバーを移転し、サービスを再開させたことが確認された。DDOS-GUARD は陰謀論運動 QAnon や 8chan のコンテンツの他、ハマスといったテロリストグループの公式サイトなどをホスティングしており、フィッシングのターゲットとされた事業者からの削除要求に従わないことから、サイバー犯罪者たちに積極的に利用されている。

新しい Robin Banks は管理インターフェースを別のサイバー犯罪者からハッキングされることを防ぐために、利用者がログインする際、多要素認証を要求するなどプラットフォームのセキュリティを強化している。

【フィッシングツールの進化】

Robin Banks は、さまざまなセキュリティ対策を回避するよう、フィッシングツールも進化させている。このツールには、アフィリエイト・マーケティングに使用される「Adspect」[39]が含まれていることが分かった。Adspect は、機械学習技術で Web サイトへの不要な訪問者を検出し、フィルタリングするためのツールであり、成功報酬型広告で稼ぐ Web サイトで一般的に使われている。Robin Banks は、フィルタリングによって、ターゲットのみをフィッシングサイトに誘導し、セキュリティソフトのクローラーを正規サイトに誘導することでフィッシングサイトの検出を回避している。これにより、セキュリティソフトを導入しているターゲットであってもフィッシングサイトに誘導することができ、また、セキュリティ企業が提供するフィッシングサイトのブラックリストにも載りにくくなると考えられる。

また、多要素認証（MFA）の普及が進んだことにより認証情報だけではログインできなくなりつつある。Robin Banks は、MFA を回避する AiTM (Adversary-in-The-Middle)フィッシング攻撃を行うコースを追加し、月額 1,500 ドルで販売している。

図 13　Robin Banks の AiTM フィッシング攻撃コースの案内

[39] 出典：Adspect『Adspect: Cloaker, Bot Filter, and Ad Tracker』
https://www.adspect.ai

3.5. まとめ

PhaaS の登場によって、フィッシング攻撃の実行と、フィッシングキットの作成やフィッシングサイトの運用が分業できるようになった。PhaaS の中でも Robin Banks は、多要素認証を回避する AiTM フィッシング攻撃のような高度な手法を実行可能とするため、技術レベルが低いサイバー犯罪者らの参入障壁が低くなっている。また、Robin Banks は、多要素認証を導入している企業等のネットワークへ侵入するために効率的なサービスであり、ランサムウェア攻撃者や APT などにも今後利用される可能性が考えられる。

Robin Banks のような PhaaS の利用が広がり、多要素認証の安全性は低下する状況が想定される。防御側は FIDO 認証等の更なる対策を進めることが要求されるであろう。

以上

免責事項

本記事の内容は、正確であることに最善を尽くしておりますが、内容を保証するものではなく、本記事の利用に起因して発生したいかなる損害、損失についても補償しませんのでご留意ください。記事内に誤植や内容の誤り、その他ご指摘等、お問い合わせ事項がある場合は、お手数ですが下記までご連絡ください。

お問い合わせ先：NTT セキュリティ・ジャパン株式会社

コンサルティングサービス部　OSINT モニタリングチーム
メールアドレス： WA_Advisorysupport@ntt.com