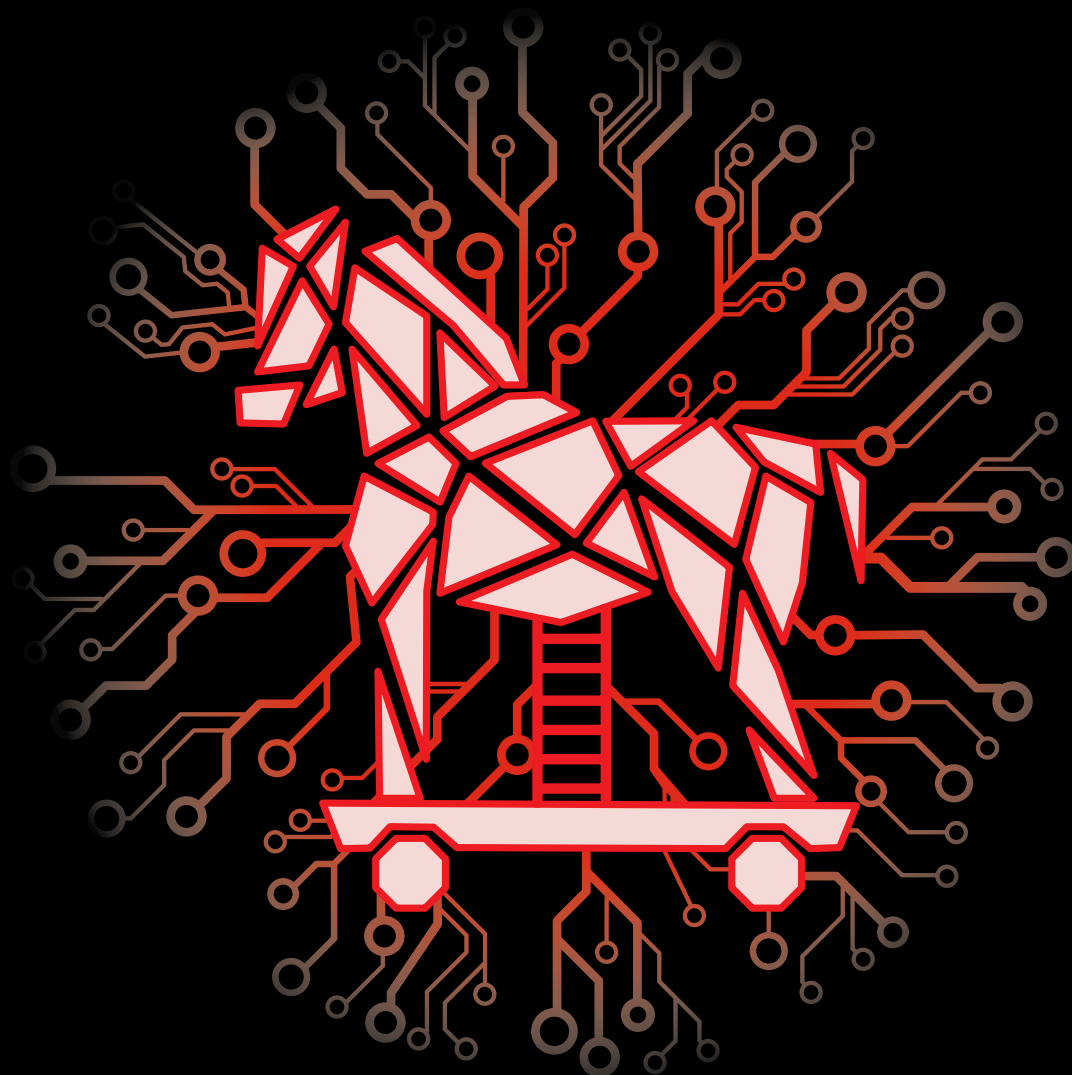


Deloitte.

デロイトトーマツ



Red Team Operations
Attackers Report 2020

攻撃者が分析する

Red Team Operations

Red Team Opeartaions (RTO) と日本のトレンド2020	1
業界に関する洞察、契約タイプ、および対応の概要	2
攻撃者のパフォーマンスとクライアントのレジリエンシー	3
業界別および契約タイプ別のクライアントのレジリエンシー	6
Contacts	7

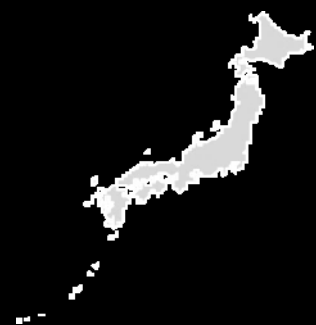
Red Team Operations (RTO) と日本のトレンド2020



COVID-19が及ぼす
セキュリティ監視や
インシデントレスポ
ンスへの影響

コロナウイルス (COVID-19) の感染拡大により爆発的に増加したリモートワーク環境に対するセキュリティ上の懸念から、日本を含む世界では自社のセキュリティ対策の有効性の確認を求められるケースや、今後懸念が増加すると予想されるエンドポイント対策や端末感染時の監視体制、インシデントレスポンスの有効性にフォーカスを当てた評価を当社のRed Teamと共に確認するニーズが増え始めています。

脅威ベースのペネトレーションテスト (TLPT) を実施するクライアントの増加



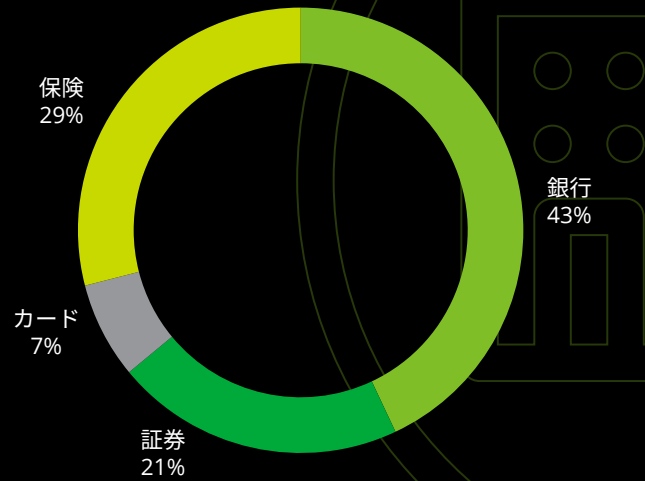
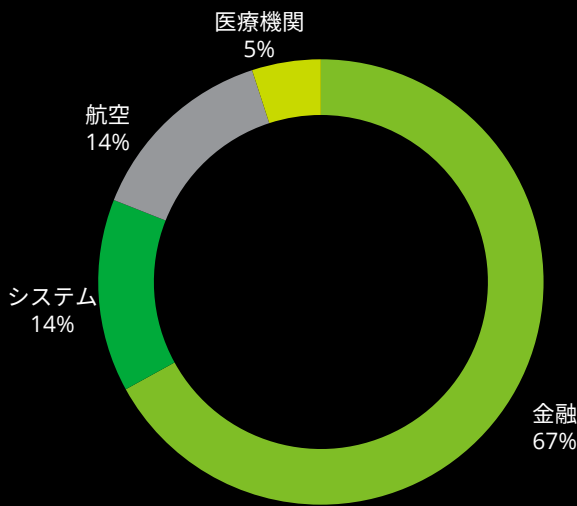
2018年10月に金融庁が発行した、金融分野におけるサイバーセキュリティ強化に向けた取組方針に脅威ベースのペネトレーションテストの実施が明記されました。これを機にTLPTの実施を求めるクライアントが増加しており、2019年はRTOよりもTLPTの実施数が上回る結果になりました。

業界に関する洞察、契約タイプ、および対応の概要

Red Teamを実施した実績のあるクライアントの業態割合

日本国内の実績としては金融業界の割合が最も高くなっています。

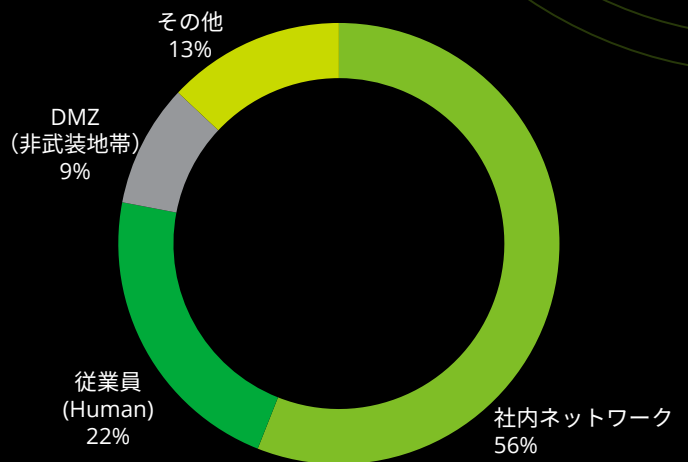
金融業界の中では銀行向けに実施しているケースが40%以上と多く、続いて保険、証券、カード会社に対し、Red Team Operationsに関連した評価を実施しています。



攻撃対象の割合

従業員の業務端末がマルウェアに感染したケースを想定し、OA環境を主な評価の対象とするのが主流になっています。また、昨今ではフィッシングメールを起点としたOA環境の評価等、攻撃対象の範囲に従業員 (Human) の要素を含めるケースが増えつつあります。

また脅威情報と絡めて攻撃対象を定めるようなケースも今後増えてくる見込みです。



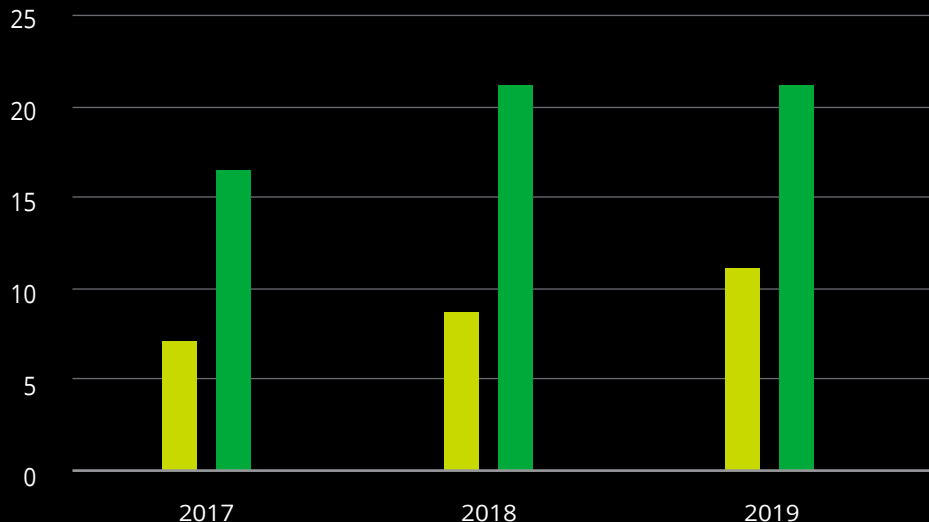
攻撃者のパフォーマンスとクライアントのレジリエンシー

ローカル、ドメイン管理者を巡る攻防

原則として、攻撃目標の達成においてローカル管理者やドメイン管理者等の特権アカウントの取得は避けて通れません。これまで行ってきた評価の傾向として、組織のセキュリティ成熟度と当チームがこれらの権限を取得するために必要な時間には相関関係があり、平均以上に時間を要するケースは攻撃者の活動を制限する対策が有効に機能した結果と言えます。

年ごとの変化ではドメイン管理者権限の取得に要する時間は、増加しています。それは、クライアントの防御チームがより高度になり、組織は、より回復力がついてきています。ローカル管理者権限を取得する時間も伸びており、変化がみられます。

企業の多くはMicrosoft Windows® をベースとした環境を構築しているため、ローカル管理者やドメイン管理者の取得に要する平均時間というのは最も重要な基準の1つになります。ただし、これは唯一の基準ということではなく、信頼できる1つの基準に過ぎません。年ごとに見られるような差異は画期的なセキュリティ対策や監視策の登場、新しい深刻な脆弱性の発見等にも影響するため右のグラフに見られるような傾向は数年で変化するでしょう。



■ ローカル管理者権限取得に要する平均時間 (時間)
■ ドメイン管理者権限取得に要する平均時間 (時間)

ローカル、ドメイン管理者権限取得率

ローカル、ドメイン
管理者共に

96%

※クラウンジュエルの達成に
ローカル、ドメイン管理者権
限が必要ない場合を除く

攻撃者のパフォーマンスと クライアントのレジリエンシー

攻撃目標の達成率

当チームではRed Team Operationsに関連する評価の94%で1つ以上の攻撃目標を定められた期間内に達成しています。

なお、攻撃目標はクライアントと当チームとの協議によって定められるため、評価ごとに設定される攻撃目標は異なります。

クライアントが選択する攻撃目標例

機密情報
(ダミーファイル)
の窃取

特定経路 (例: OA環境
からDMZ環境等)
の識別

定められたデータの
外部送付

特定環境への
アクセス

Active Directory
サーバの掌握

攻撃者のパフォーマンスと クライアントのレジリエンシー

評価毎に識別される発見事項の平均数

当チームでは、平均して8.5件ほどの発見事項をクライアントに報告しています。

ただし、複数回同様の評価を実施しているクライアントは、以前に識別された課題を改善していることからセキュリティの成熟度が向上しており、識別される発見事項の数が前年度より少なくなる傾向になるようです。

クライアントへ報告する発見事項例

特権アカウント
の管理不備

脆弱なパスワード
の利用

不十分な
モニタリング

ネットワークアクセス
制御の不備

サポートが終了した
OSやアプリケーション
の利用

業界別および契約タイプ別のクライアントのレジリエンシー

これまでにRed Team Operationsに関連した評価を実施してきたクライアントの業態別に、ローカル、ドメイン管理者権限の取得に要した時間を比較したところ、重要インフラに分類されるような企業はその他の業態と比べてセキュリティの成熟度が高い傾向にありました。



Contacts

野見山雅史 (Masafumi Nomiya)
masafumi.nomiya@tohatsu.co.jp

Ari Davies
ari.davies@tohatsu.co.jp

Carlo Emmanuele Geraci
carlo.geraci@tohatsu.co.jp

デロイト トーマツ サイバー合同会社

Mail ra_info@tohmatsumatsu.co.jp

URL www.deloitte.com/jp/dtscy

【国内ネットワーク】東京・名古屋・福岡

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイト トーマツ合同会社ならびにそのグループ法人(有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ 税理士法人、DT 弁護士法人およびデロイト トーマツ コーポレート ソリューション合同会社を含む)の総称です。デロイト トーマツ グループは、日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約30都市以上に1万名を超える専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト(www.deloitte.com/jp)をご覧ください。

Deloitte (デロイト) とは、デロイト トウシュ トーマツ リミテッド (“DTTL”)、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人 (総称して “デロイト ネットワーク”) のひとつまたは複数を指します。DTTL (または “Deloitte Global”) ならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTL および DTTL の各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。DTTL はクライアントへのサービス提供を行いません。詳細は www.deloitte.com/jp/about をご覧ください。

デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市 (オークランド、バンコク、北京、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む) にてサービスを提供しています。

Deloitte (デロイト) は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリー、リスクアドバイザリー、税務およびこれらに関連するプロフェッショナルサービスの分野で世界最大級の規模を有し、150を超える国・地域にわたるメンバーファームや関係法人のグローバルネットワーク (総称して “デロイト ネットワーク”) を通じ Fortune Global 500® の8割の企業に対してサービスを提供しています。“Making an impact that matters” を自らの使命とするデロイトの約312,000名の専門家については、(www.deloitte.com) をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、デロイト トウシュ トーマツ リミテッド (“DTTL”)、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人 (総称して “デロイト ネットワーク”) が本資料をもって専門的な助言やサービスを提供するものではありません。皆様の財務または事業に影響を与えるような意思決定または行動をされる前に、適切な専門家にご相談ください。本資料における情報の正確性や完全性に関して、いかなる表明、保証または確約 (明示・黙示を問いません) をするものではありません。またDTTL、そのメンバーファーム、関係法人、社員・職員または代理人のいずれも、本資料に依拠した人に関係して直接また間接に発生したいかなる損失および損害に対して責任を負いません。DTTLならびに各メンバーファームおよびそれらの関係法人はそれぞれ法的に独立した別個の組織体です。

Member of
Deloitte Touche Tohmatsu Limited

© 2020. For information, contact Deloitte Tohmatsu Cyber LLC.