

Red Team Operations
Attackers Report 2020
Overview of key
engagement results

Red Team Operations (RTO) Global and Japan trends 2020	1
Industry insights, engagement types and response overview	2
Attacker performance and Client resiliency	3
Client resiliency by industry and engagement types	6
Contacts	7

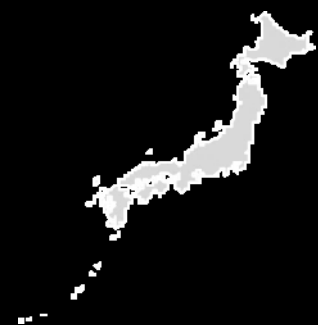
Red Team Operations (RTO) Global and Japan trends 2020



Covid-19 will reshape the focus of incident response and monitoring

Due to the dramatic increase in remote telework as result of the COVID-19 outbreak, our clients are increasingly concerned about the cyber security implications of remote work environments and whether their existing security controls are still effective. Clients are including in the scope of their Red Teaming engagements scenarios to assess their security solutions, monitoring teams and incident response procedures with a particular focus on remote work systems and endpoint security.

In Japan, we are expecting an increase in the demand of Threat-Led Penetration Testing (TLPT)



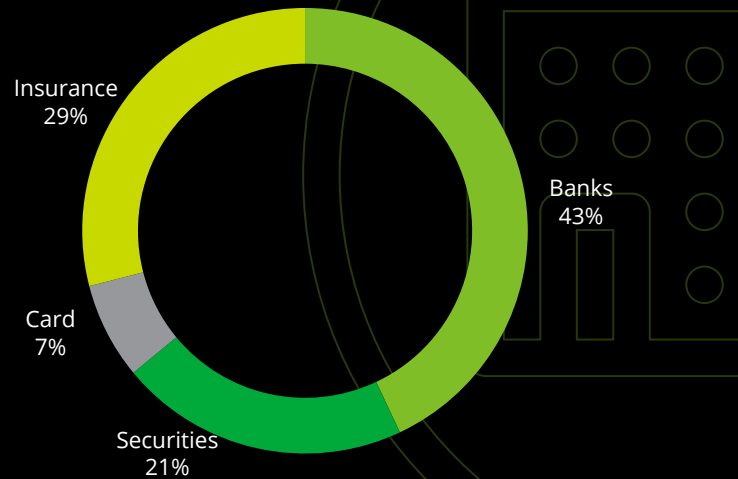
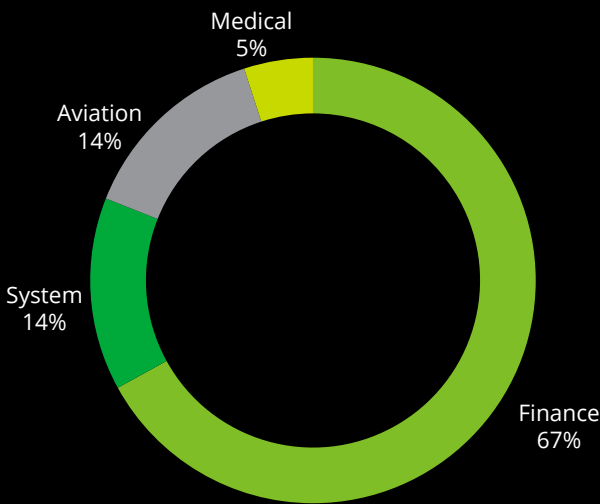
In October 2018, the Financial Service Agency of Japan has set out a number of initiatives to highlight the need for Threat Led Penetration Testing to reinforce Japan's cyber security capabilities. Because of this, we have seen a steady increase in the demand of TLPT projects.

Industry insights, engagement types and response overview

Engagement activities by Industry in Japan

In Japan, the majority of RTO engagements are provided to the Financial Services Industry (FSI).

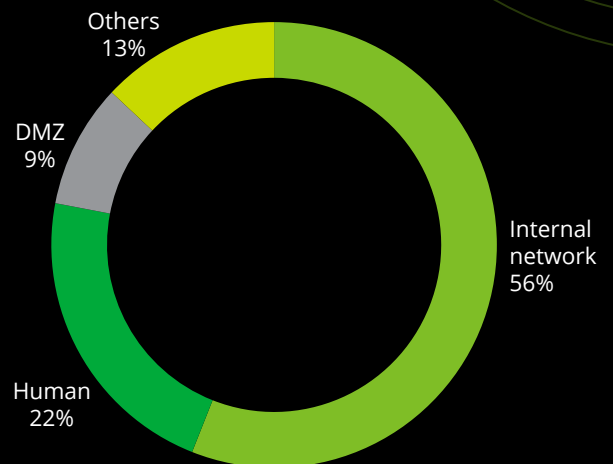
Within FSI, the Banking sector comprises the highest percentage of RTO projects - with over 40% of the engagement share.



Key Engagement Targets

Clients have been focusing on their internal network protection when engaging Deloitte in Japan. These engagements typically start from a client's workstation.

Human aspects of cyber resiliency are often tested by using phishing campaigns targeting company employees as an entry point to infiltrate the environment.



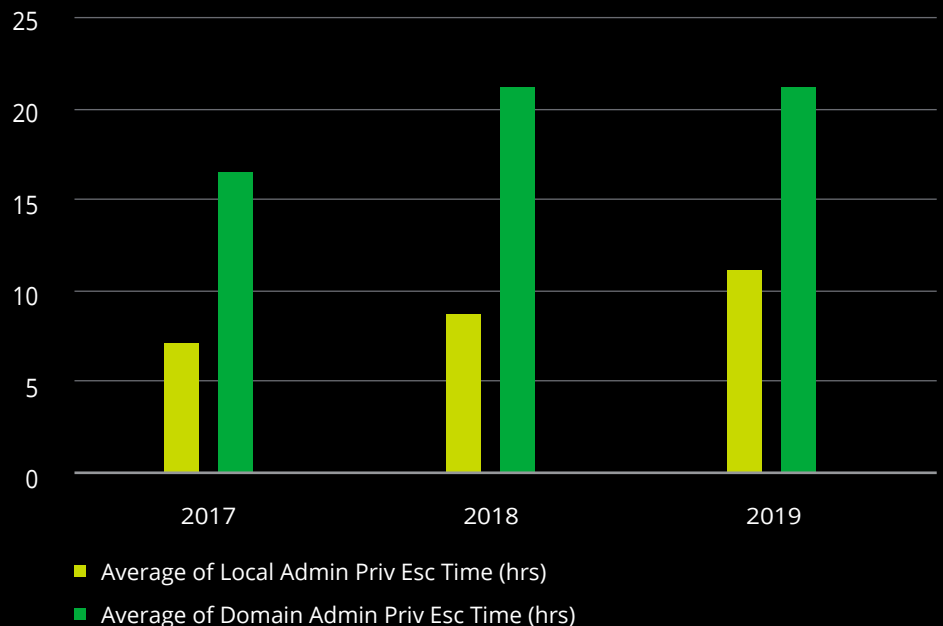
Attacker performance and Client resiliency

Local Admin and Domain Admin Privileges

It is common, during RTO engagements, to have as primary or secondary objectives the need to obtain local and domain admin privileges. The time our team needs to gain these credentials is usually indicator of the cyber maturity level of an organisation.

Across all sectors the time our team needs to obtain administrative level privileges is increasing, which is a sign that the defensive teams of our clients are becoming more advanced and their organizations are becoming more resilient.

Since most organisations use Microsoft Windows® based environments, one of the most important metrics is the average time to Local and Domain Administrative privileges. While this is not the only metric, it is a reliable one. Overall we have noticed that the advantage is constantly switching between the blue and red team as time progresses and that with more testing and practice the defensive teams of our clients are becoming better.



How often do we get in?

96%
of the time

Excludes engagements where obtaining Local/Domain Admin privileges is not required

Attacker performance and Client resiliency

How far do we usually get?

Within the engagement window we have a success rate of 94% of obtaining the crown jewel objectives.

Crown jewels are personalised to each client and engagement and are defined in the initial client discussions between the client and Deloitte since they are defined in the initial discussion between the client and the RTO team.

Typical Crown Jewels chosen by our Clients

Obtain confidential information within a restricted folder

Exfiltrate data from the network

Obtain Domain Controller full access

Obtain employee credentials

Obtain specific environment access

Attacker performance and Client resiliency

How many issues do we usually find?

Clients who have an ongoing security assessment relationship with us have benefited by implementing the recommendations we have made over the years. This reduces the number of vulnerabilities and weaknesses which can be exploited by an attacker.

On average, our team discovers **between three and seventeen** issues during each engagement that are reported to the client.

Typical issues reported to Clients

Insufficient management for privileged accounts

Weak password configurations

Insufficient monitoring

Insufficient network access control

Legacy applications or OS

Client resiliency by industry and engagement types

On average, by industry, Insurance and Aviation (Airports) appear to be more resilient during RTO engagements. By comparison Healthcare clients (hospitals) required the least amount of time for our team to gain privileged access.



Contacts

Masafumi Nomiya

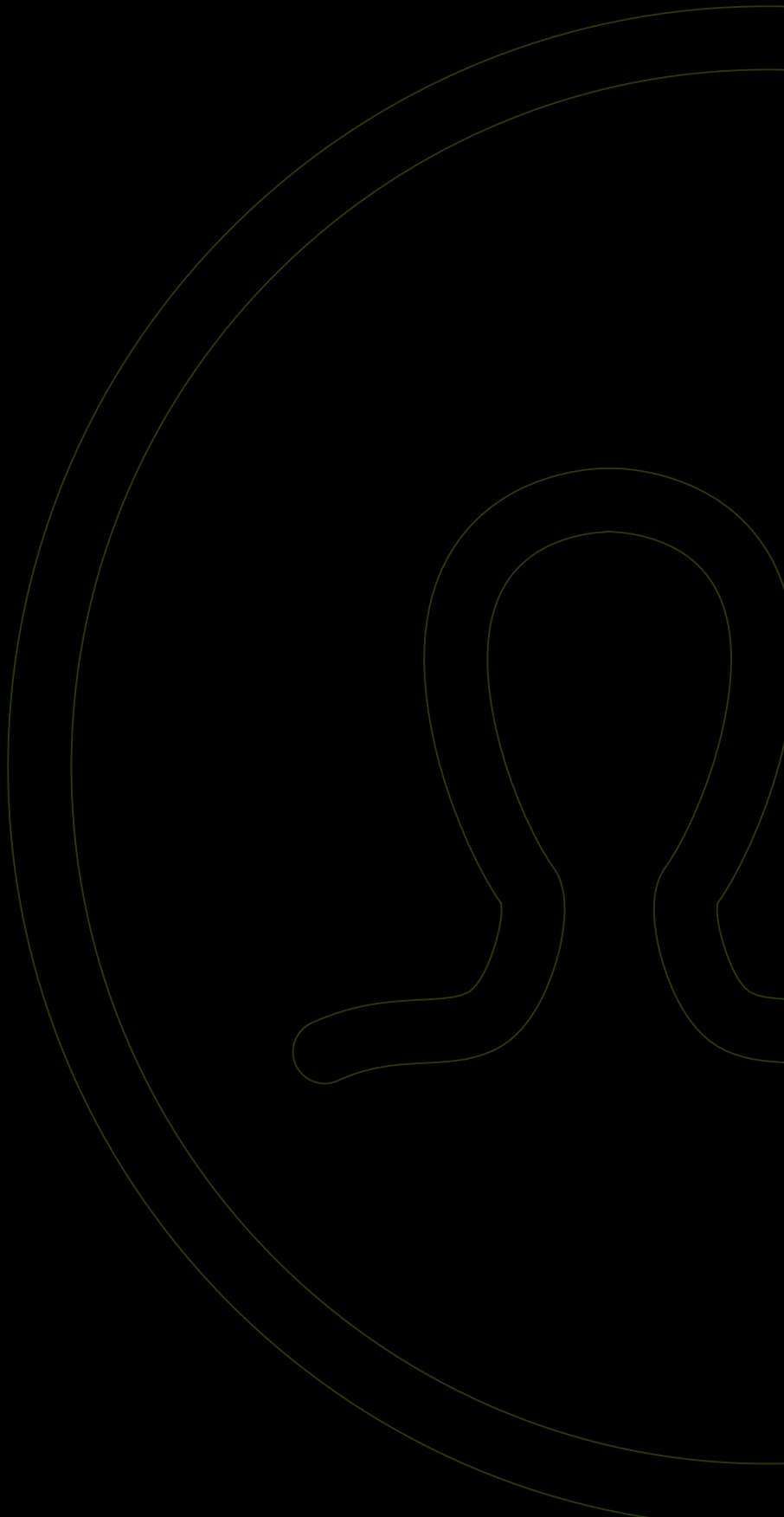
masafumi.nomiya@tohatsu.co.jp

Ari Davies

ari.davies@tohatsu.co.jp

Carlo Emanuele Geraci

carlo.geraci@tohatsu.co.jp



Deloitte Tohmatsu Cyber LLC

Mail ra_info@tohatsu.co.jp

URL www.deloitte.com/jp/en/dtcy

Deloitte Tohmatsu Group (Deloitte Japan) is a collective term that refers to Deloitte Tohmatsu LLC, which is the Member of Deloitte Asia Pacific Limited and of the Deloitte Network in Japan, and firms affiliated with Deloitte Tohmatsu LLC that include Deloitte Touche Tohmatsu LLC, Deloitte Tohmatsu Consulting LLC, Deloitte Tohmatsu Financial Advisory LLC, Deloitte Tohmatsu Tax Co., DT Legal Japan, and Deloitte Tohmatsu Corporate Solutions LLC. Deloitte Tohmatsu Group is known as one of the largest professional services groups in Japan. Through the firms in the Group, Deloitte Tohmatsu Group provides audit & assurance, risk advisory, consulting, financial advisory, tax, legal and related services in accordance with applicable laws and regulations. With more than 10,000 professionals in over 30 cities throughout Japan, Deloitte Tohmatsu Group serves a number of clients including multinational enterprises and major Japanese businesses. For more information, please visit the Group's website at www.deloitte.com/jp/en.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organization") serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 312,000 people make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

Member of
Deloitte Touche Tohmatsu Limited

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