

IT FORENSIC

Kejahatan Digital

Adrian

Muhammad Rizky Rivaldo



Daftar Isi

Bahan Diskusi

Kebocoran Data
Pada PT Asuransi
BRI Life

REvil Ransomware
Attack on Kaseya

Topic 1

KEBOCORAN DATA PADA PT ASURANSI BRI LIFE



Pengenalan

BRI Life merupakan anak usaha dari BRI yang bergerak di bidang **asuransi jiwa.**



Case

Pada tahun 2021 sekitaran bulan Juni atau Juli. Terjadi kebocoran data yang mengakibatkan sekitar 250 GB yang berisis **2 juta data nasabah dan 463.000 dokumen** terekspos oleh pihak yang tidak diketahui dan dijual di darkweb seharga \$7000 atau sekitar Rp Rp 101,5 juta.



Foto KTP



Nomor Rekening



KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PAJAK

NPWF XX.YYY.Z.XXX.YYY

Nama 1 2 3 4 5

NIK : XXXXX.2XXXXXX.5

Alamat : Jl. No. RT. RW.

Kel. Kec. Kab.

Prop.

KPP : Pratama ABC

Nomor wajib pajak



Akte Kelahiran

Data Rekam Medis

13 Mei 2020 - 11 Juni 2020

Id Rekam Medis	Nama Pasien	Nama Dokter	Tanggal Periksa
RM2020061100003	Pasien 5	Dokter 1	11 Juni 2020
RM202006100001	Pasien 1	Dokter 2	10 Juni 2020
RM202006110001	Pasien 3	Dokter 3	11 Juni 2020
RM202006100002	Pasien 2	Dokter 4	10 Juni 2020
RM202006110002	Pasien 4	Dokter 4	11 Juni 2020
RM202006110004	Pasien 6	Dokter SourceCodeKu.com	11 Juni 2020

Data rekam Medis

Kronologis

- 1** Pada tanggal 27 Juli 2021, pengguna akun twitter @underthebreach, mengirimkan sebuah video berdurasi 30 menit yang berisikan data sebesar 250 GB yang berisi data - data nasabah BRI Life dibocorkan dan dijual di situs tidak resmi. Bisa saja kebocoran kasus tersebut lebih lama dari tanggal underthebreach memberitahukan informasi ini.
- 2** Pada tanggal yang sama pihak BRI Life dan lembaga keamanan informasi lainnya segera menyelidiki kasus dan menduga data tersebut bocor karena peretas berhasil membobol komputer karyawan
- 3** Pada tanggal 29 Juli, pihak BRI Life, Kominfo, OJK, Kementerian informasi dan komunikasi dan pihak lainnya sudah menyelidiki kasus. pihak BRI mengatakan kalau data yang bocor tersebut tidak dimanipulasi atau dipalsukan karena menggunakan sistem stand alone.
- 4** Tanggal 30 Juli, situs tempat data dijual telah dihapuskan, akan tetapi pelaku kejahatan masih belum terungkap hingga sekarang.

DAMPAK DAN PERANGKAT

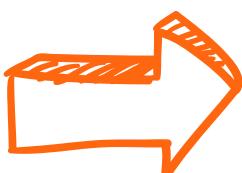


Sisi Baik

Tidak ada data yang salah digunakan.

Sisi Buruk

Nama baik BRI Life menjadi buruk.



Hal yang perlu diketahui

BAGAIMANA CARA KERJA ASURANSI?

The diagram consists of five dark grey circles connected by purple curved lines, forming a horizontal sequence. Each circle contains text describing a step in the insurance process:

- Nasabah
- Ajukan klaim
- Perusahaan asuransi
- Cek kelengkapan dokumen
- Jika disetujui, pencairan klaim

MUNGKINKAH KLAIM TIDAK DISETUJUI?

MUNGKIN, JIKA NASABAH TAK MEMBERIKAN DOKUMEN YANG DIBUTUHKAN.

<https://www.cnnindonesia.com/tag/hasnaeni-wanita-emas>

HD +

CNN
Indonesia

Jadi sebenarnya
data nasabah
itu aman aman
saja, karena



- 01.** Dokumen harus lengkap
- 02.** Data tersebut tidak terjual
- 03.** Situs tersebut sudah dihapus

Topic 2

REvil Ransomware Attack on Kaseya



Apa itu Ransomware ?

**Tipe Malware yang
mengenkripsi data
korban kemudian
meminta uang tebusan
untuk memulihkannya**



IT MANAGEMENT & SECURITY

**Mengembangkan software
yang mengatur jaringan,
sistem, dan infrastruktur
teknologi informasi.**

FUNCTION



Kronologis Penyerangan

2 JULI 2021

Menerima laporan penyerangan dan langsung mematikan seluruh server

4 JULI 2021

REvil mengklaim penyerangan dan hasil diskusi diserahkan kepada Internet Complaint Centre

3 JULI 2021

Compromise Detection Tool untuk pelanggan

9 JULI 2021

Joe Biden menginformasikan kepada Vladimir Putin

8 OKTOBER
2021

Dua Pelaku tertangkap yaitu Yaroslav Vasinskyi dan Yevgeniy Polyanin di Polandia



REvil Ransomware

Time - Impact - Device



WAKTU PENYERANGAN

2 Juli 2021

Pukul 2:00 PM EDT



DAMPAK

Sebanyak 50 pelanggan Kaseya terkena, dimana dari 50 pelanggan tersebut memiliki 800-1500 bisnis dibawahnya

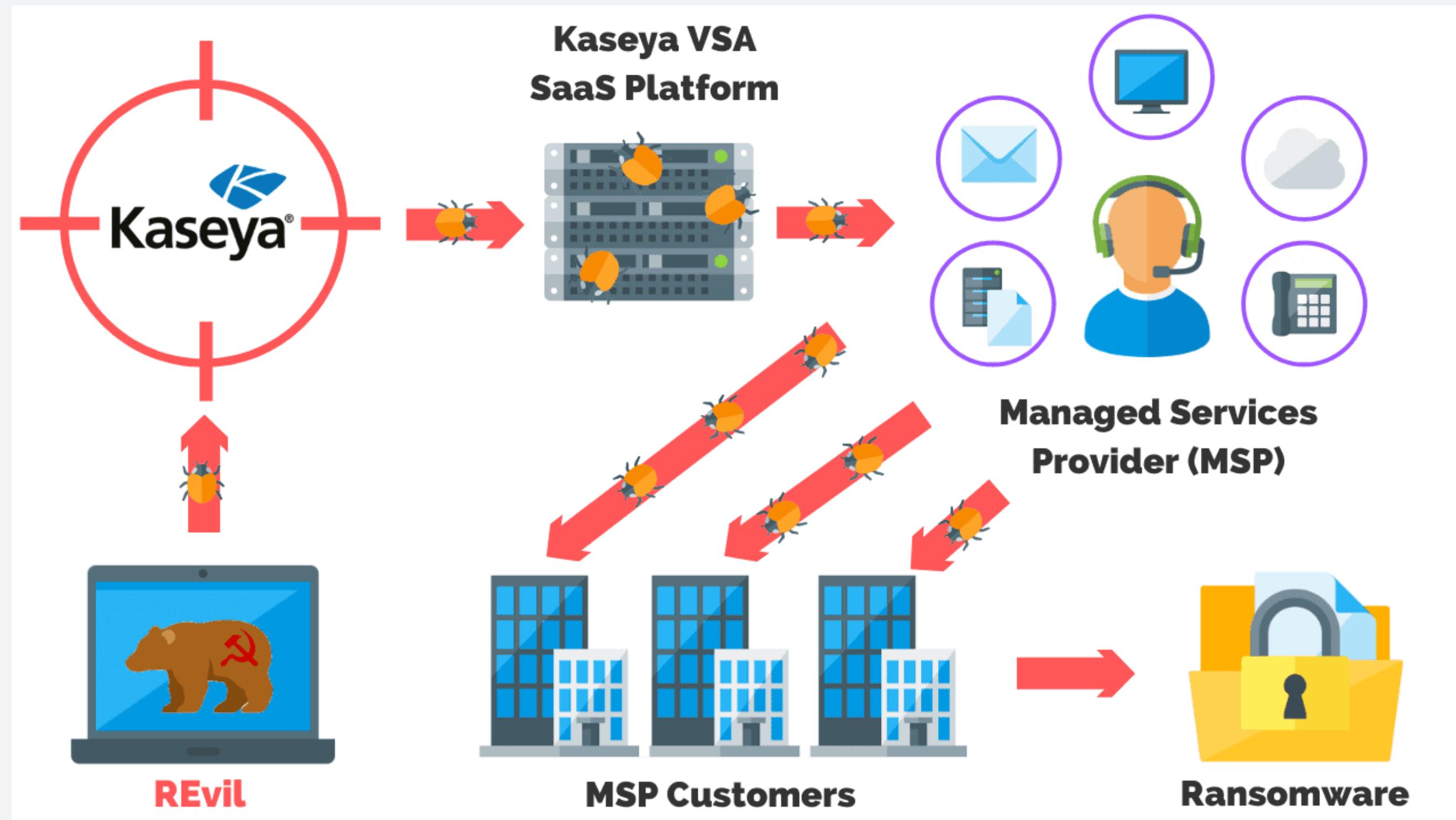


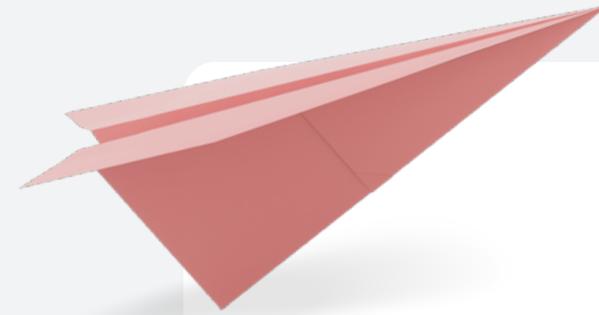
DEVICE YANG DIGUNAKAN / TERKENA

Laptop

Komputer

Cash Register





**Do you have any
questions?**

