

Peningkatan Kesadaran dan Pencegahan Serangan Ransomware dan Virus

Versi Video:

Klik pada video untuk memulai. Double-click untuk memperbesar tampilan video. Tersedia suara narator dan caption.

Versi Teks:

Yth. Bapak/Ibu,

Akhir-akhir ini, serangan virus dan ransomware yang menyasar perusahaan dan institusi, baik swasta maupun pemerintah, kembali marak terjadi. Sebagai contoh, serangan ransomware baru-baru ini menimpa server PDN (Pusat Data Nasional) di lingkungan KOMINFO (Kementerian Komunikasi dan Informatika) dengan varian ransomware Brain Cipher.

Apa itu ransomware dan Brain Cipher Ransomware?

Ransomware adalah jenis malware yang digunakan peretas untuk menyandera data penting milik korban, baik individu maupun korporasi, dengan mengenkripsi data tersebut. Pelaku kemudian akan meminta tebusan berupa uang, termasuk cryptocurrency seperti Bitcoin.

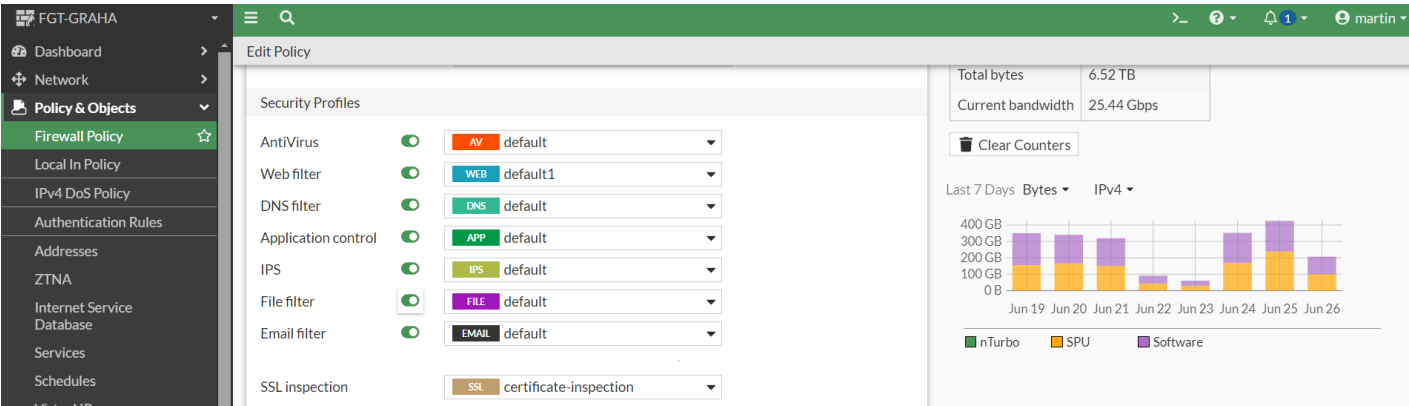
a. Brain Cipher Ransomware adalah geng peretas yang menggunakan varian ransomware Lockbit untuk menyerang sistem korban, menurut Broadcom, penyedia layanan keamanan siber Symantec. Informasi lebih lanjut dapat ditemukan di <https://kumparan.com/kumparantech/apa-itu-brain-cipher-ransomware-yang-bikin-lumpuh-server-pdn-kominfo-2302QtPRjyx/4> .

b. Brain Cipher Ransomware adalah jenis ransomware baru yang muncul tahun ini. Ransomware ini mengenkripsi file korban dan meminta tebusan sebagai ganti kunci dekripsi. Peretas biasanya menyebarkan email phishing atau unduhan berbahaya, mengeksploitasi kerentanan dalam sistem untuk mendapatkan akses. Serangan ini menggunakan teknik canggih untuk menyusup, menyebar, dan mengenkripsi data dalam jaringan yang ditargetkan. Metode pengiriman utamanya adalah melalui email phishing, yang sering kali berisi lampiran atau tautan berbahaya yang mengarah ke unduhan malware. Informasi lebih lanjut dapat ditemukan di <https://katadata.co.id/digital/teknologi/66796641b9261/apa-itu-brain-cipher-ransomware-yang->

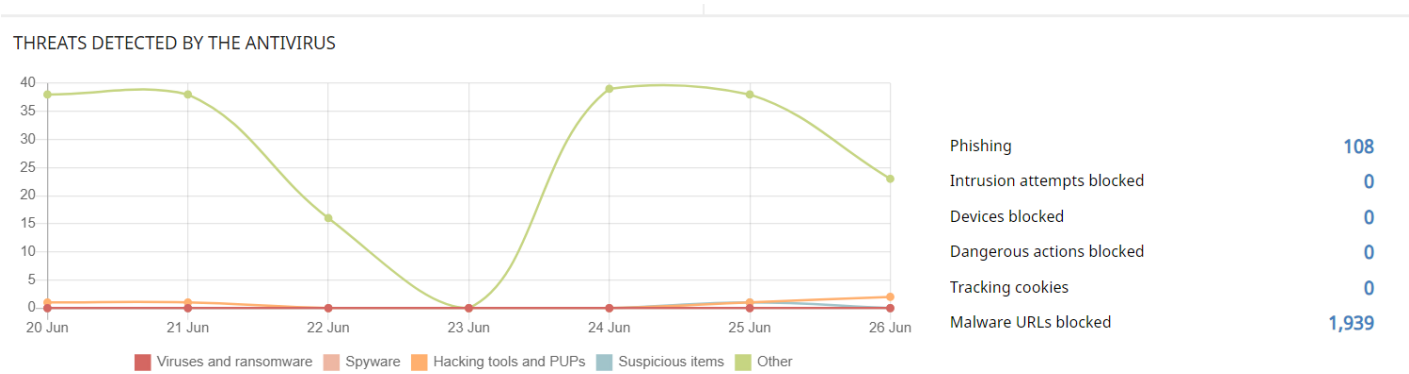
serang-pusat-data-nasional .

Untuk mencegah serangan ransomware dan virus lainnya, langkah-langkah yang telah diterapkan di lingkungan MBF meliputi peningkatan keamanan jaringan yang berlapis dengan menggunakan firewall dan antivirus.

1. **Firewall:** Penggunaan firewall diterapkan mulai dari masuknya koneksi internet ISP yang difilter perangkat firewall untuk menyaring data masuk mulai dari antivirus, web, aplikasi, file, sampai email filter.



2. **Antivirus:** Di layer end-user, selain antivirus layer jaringan, MBF juga menggunakan antivirus yang diinstal di PC dan laptop. Antivirus ini mendeteksi virus, ransomware, spyware, hacking tools, dan Potentially Unwanted Programs (PUP).



3. **Backup Data:** Backup data server dilakukan secara periodik. Backup data dari server produksi, database, email, web, dan file server disimpan di server Linux yang lebih aman dari serangan virus.

Veeam Backup and Replication

Home View Job

Start Stop Retry Active Full Statistics Report Edit Clone Disable Delete

Job Control Details Manage Job

Home

Jobs

- Backup
- Backup Copy
- Backups
- Disk
- Disk (Copy)
- Last 24 Hours
- Success

Home

Inventory

- Backup Infrastructure
- Storage Infrastructure
- Tape Infrastructure

Type in an object name to search for

All jobs

Name	Type	Objects	Status	Last Run	Last Result
App LIVE Daily 1X HRIS App	Windows Agent Backup	1	Stopped	12 hours ago	Success
App LIVE Daily 1X IA-FOXPRO	Windows Agent Backup	1	Stopped	12 hours ago	Success
App LIVE Daily 1X IA-Web App & DB	Windows Agent Backup	1	Stopped	12 hours ago	Success
App LIVE Daily 1X Web App	Windows Agent Backup	1	Stopped	12 hours ago	Success
Backup Copy	Backup Copy	20	Stopped	19 minutes ago	Success
DB LIVE Daily 2X - Navision	Windows Agent Backup	1	Stopped	1 hour ago	Success
DB LIVE Daily 3X HRIS	Windows Agent Backup	1	Stopped	1 hour ago	Success
DB LIVE Daily 3X L2/L3	Windows Agent Backup	1	Stopped	27 minutes ago	Success
DB LIVE Daily 3X Web	Windows Agent Backup	1	Stopped	58 minutes ago	Success
Linux Web Server Daily Backup	Linux Agent Backup	1	Stopped	10 hours ago	Success
NAS Server LIVE Daily 2X NAS-2 Graha	Windows Agent Backup	1	Stopped	31 minutes ago	Success
NAS Server LIVE Daily 2X NAS-5 Plant	Windows Agent Backup	1	Stopped	26 minutes ago	Success
TOOLS - Daily 1X IA Active Directory	Windows Agent Backup	1	Stopped	14 hours ago	Success
TOOLS - Daily 1X MBF Active Directory	Windows Agent Backup	1	Stopped	14 hours ago	Success

SUMMARY

Duration: 04:34

Processing rate: 12 GB/s

Bottleneck: N/A

DATA

Processed: 3.1 TB (100%)

Read: 0 B

Transferred: 0 B

STATUS

Success: 1

Warnings: 0

Errors: 0

THROU

id: 0 KB

Namun demikian, selain semua usaha preventif yang sudah dilakukan, kami juga mengharapkan peran serta dari seluruh user MBF untuk selalu waspada dan berhati-hati, terutama ketika menggunakan jaringan internet di kantor. Hindari mengakses atau membuka link yang diperoleh dari web atau email secara sembarangan. Jika membawa flash disk dari luar, harap selalu melakukan pemindaian terlebih dahulu.

Khusus untuk email, jika menerima email, jangan sembarang membuka lampiran atau mengklik link atau tombol yang ada di dalam email tersebut. Banyak email yang tampak valid tetapi sebenarnya mengandung virus dan link ransomware. Jika menerima email yang mencurigakan, harap segera menghapusnya dan jangan mengklik tautan yang ada di dalam email tersebut. Apabila ragu, silakan menanyakan terlebih dahulu ke IT Support.

Action is Required on martin.widjaja@mbf.co.i...



From **cPanel E-mail Administrator** 
To **martin.widjaja@md@nti.edu.pk**
Date **2024-06-11 06:54**

Arahkan kursor pada Nama,
nanti muncul alamat email
pengirim, TIDAK DIKENAL

Sent from a trusted sender.

Walaupun ada kata-kata ini.

Hello **martin.widjaja@mbf.co.id**,

You have 14 emails pending.

Follow the link below to release it all to your inbox.

RELEASE NOW

Regards

Jangan pernah klik tombol atau link pada email yang mencurigakan

mbf.co.id cPanel Security Gateway

This is a service notification and does not mean you will receive mass mailings from us.

This message is auto-generated from Drakephilippines Security Gateway; replies sent to this email cannot be delivered.

Copyright © 2024 Inc. All rights reserved

Mari kita bersama-sama peduli, teliti, disiplin, dan saling menjaga terkait data perusahaan.

Demikian himbauan dan informasi dari kami. Jika masih belum paham, jangan sungkan untuk bertanya ke Tim IT Support.

Revision #5

Created 28 June 2024 07:30:52 by Martin

Updated 28 June 2024 07:48:51 by Martin