Monitoring Infrastruktur Teknologi Informasi, Garda Terdepan Menjaga Keamanan Data

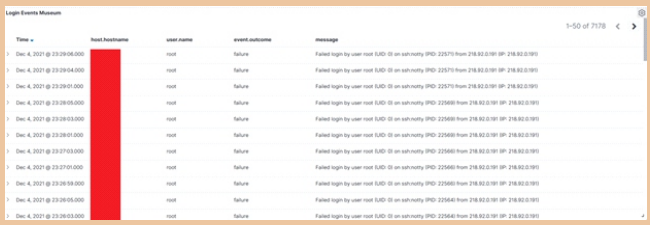
Menjaga performa pelayanan aplikasi yang ada di PUSTAKA tidak lepas dari kegiatan monitoring infrastruktur teknologi informasi seperti Server, Router, Switch, Access Point, dan Firewall. Salah satu upaya yang dilakukan adalah dengan monitoring keamanan untuk terjaganya aspek kerahasiaan, integritas, dan ketersediaan layanan digital PUSTAKA seperti website dan aplikasi lain.

Pusat Perpustakaan dan Penyebaran Teknologi Pertanian (PUSTAKA) sebagai perpustakaan pertanian terbesar di Indonesia memiliki koleksi digital yang cukup besar. Koleksi tersebut dikelola dan dilayankan kepada para pengguna melalui aplikasi berbasis web, seperti repositori pertanian, portal perpustakaan pertanian, katalog perpustakaan, serta *website* Museum Tanah dan Pertanian.

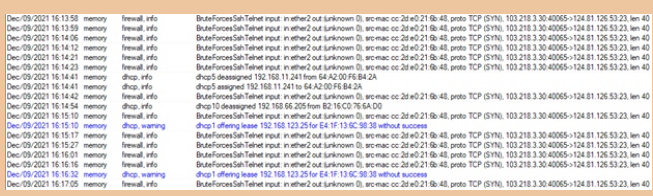
Berbicara tentang perpustakaan dan koleksi digital tidak terlepas dari isu terkait keamanan data digital. Serangan siber mungkin saja terjadi terhadap data digital yang dimiliki oleh perpustakaan khususnya PUSTAKA. Untuk menjaga keamanan data yang ada di PUSTAKA dilakukan monitoring infrastruktur Teknologi Informasi (TI) seperti *Server, Router, Switch, Access Point,* dan *Firewall* secara rutin. Keamanan infrastruktur TI merupakan garda terdepan untuk melindungi informasi digital terhadap serangan siber yang mungkin terjadi, sehingga dapat dideteksi dan dihentikan secepat mungkin. Beberapa jenis serangan yang pernah terjadi ditemukan pada infrastruktur TI adalah *brute force, privilege escalation, crawler-bot, serta directory traversal*.

Brute force

Brute force adalah sebuah tipe serangan siber dimana penyerang melakukan upaya *trial and error* untuk 'menebak' akses ke suatu *resources*. Teknik *brute force* dapat digunakan dengan memanfaatkan *user login*, kunci enkripsi, ataupun direktori pada sebuah aplikasi web. Aksi *brute force* yang dilakukan penyerang pada infrastruktur TI di PUSTAKA sendiri tergolong cukup banyak. Sebagai contoh upaya *brute force* yang tercatat pada server *website* Museum Tanah dan Pertanian pada 4 Desember 2021 dalam kurun waktu



Gambar 1. Aktifitas brute force yang terjadi pada server website Museum Tanah dan Pertanian tanggal 4 Desember 2021



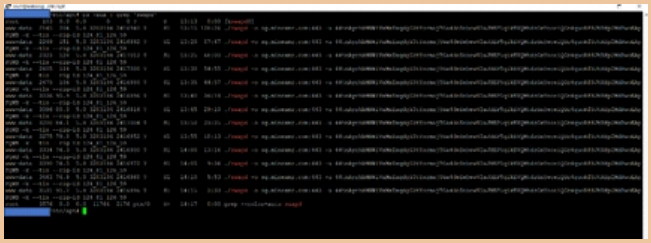
Gambar 2. Aktifitas bruteforce yang terjadi pada perangkat router PUSTAKA tanggal 9 Desember 2021

selama 24 jam terjadi sebanyak 7.178 kali percobaan, seperti dapat dilihat pada Gambar 1, selain serangan ke server, para peretas melakukan serangan *brute force* terhadap perangkat router PUSTAKA, serangan tersebut melalui *service telnet*.

Privilege Escalation

Privilege escalation adalah sebuah serangan yang dilakukan untuk mendapatkan *privilege* (hak akses) tertinggi dalam sebuah sistem (akses root), biasanya serangan ini terjadi memanfaatkan *system bug*,

miskonfigurasi, ataupun akses kontrol yang kurang memadai. Di PUSTAKA hal ini pernah terjadi satu kali, yaitu pada 29 Maret 2021, dimana penyerang mendapat akses untuk dapat menanam sebuah *crypto-miner bot* yang memanfaatkan *resources server* tersebut untuk melakukan aktivitas penambangan



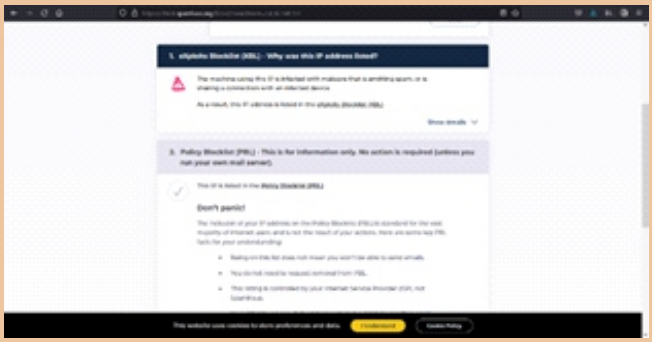
Gambar 3. *Serangan crypto-miner botnet yang memanfaatkan privilege escalation*

crypto currency. Akan tetapi serangan tersebut segera terdeteksi dan tertangani melalui analisis *log-file* sehingga tidak menimbulkan kerusakan apapun.

Crawler-bot

Crawler-bot adalah aplikasi yang mampu menjalankan tugas otomatis dan dapat bertindak layaknya orang sungguhan di jaringan internet. Aplikasi ini sebenarnya berfungsi melakukan *crawling* pada sebuah *web* secara sistematis untuk keperluan *SEO* (*Search Engine Optimization*). Akan tetapi ada orang yang memanfaatkan kemampuan yang dimiliki aplikasi tersebut untuk menggali informasi sensitif pada sebuah *website* demi kepentingan tertentu maupun untuk merusak kinerja dengan cara memenuhi *traffic* pada sebuah *website*.

Temuan malicious *crawler-bot* yang pernah terdeteksi di PUSTAKA contohnya seperti "*Ahrefbot*" dan "*Semrushbot*". *Crawler-bot* ini terdeteksi melalui



Gambar 4. Serangan crawler-bot

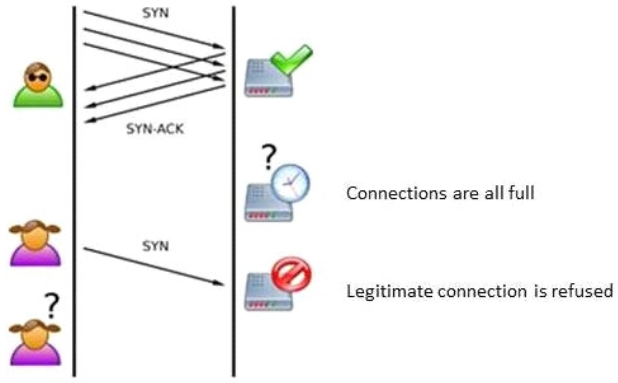
analisis *log-file* pada web server dan berdasarkan informasi pada website https://check.spamhaus.org/ yang mengelompokkan *crawler-bot* tersebut sebagai *malware*, seperti yang terlihat pada Gambar 4.

Directory Traversal

Directory Traversal adalah kerentanan yang terdapat pada sebuah aplikasi *web* yang memungkinkan *threat actor* (pengguna tidak sah) dapat mengakses file dan direktori yang berada di luar *web root* folder. Kasus *directory traversal* pernah dialami oleh PUSTAKA, salah satunya adalah pada saat informasi kerentanan pada aplikasi *apache web server* versi tertentu telah tersebar luas di internet. Dimana angka percobaan yang dilakukan *threat actor* untuk mencari celah kerentanan pada *server* PUSTAKA bertambah secara signifikan. Salah satunya terjadi pada tanggal 13

Gambar 5. Upaya pemanfaatan kerentanan yang terjadi di salah satu aplikasi PUSTAKA

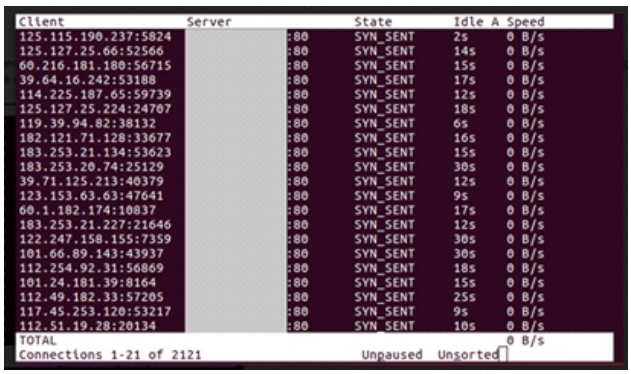
Oktober 2021 dan 4 November 2021. Seperti yang terlihat pada Gambar 5, *threat actor* mencoba melakukan serangan *directory traversal* terhadap server PUSTAKA yang menggunakan aplikasi *apache web server*.



Gambar 6. Ilustrasi Syn Flood - devcentral.f5.com

Flooding Attack

Flooding attack atau *SYN Flood* merupakan salah satu bentuk serangan *Denial of Service* (DOS) dimana penyerang mengirimkan banyak paket SYN (*Synchronize*) dengan tujuan untuk mengkonsumsi sumber daya dari server sasaran, sehingga tidak bisa melayani lalu lintas data yang seharusnya. Paket SYN merupakan salah satu jenis paket dalam protokol *Transmission Control Protocol* (TCP). TCP adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu perangkat ke perangkat lain di dalam jaringan internet.



Client	Server		State	Idle	A	Speed
125.115.190.237:5824		:80	SYN_SENT	2s		0 B/s
125.127.25.66:52566		:80	SYN_SENT	14s		0 B/s
60.216.181.180:56715		:80	SYN_SENT	15s		0 B/s
39.64.16.242:53188		:80	SYN_SENT	17s		0 B/s
114.225.187.65:59739		:80	SYN_SENT	12s		0 B/s
125.127.25.224:24707		:80	SYN_SENT	18s		0 B/s
119.39.94.82:38132		:80	SYN_SENT	6s		0 B/s
182.121.71.128:33677		:80	SYN_SENT	16s		0 B/s
183.253.21.134:53623		:80	SYN_SENT	15s		0 B/s
183.253.20.74:25129		:80	SYN_SENT	30s		0 B/s
39.71.125.213:40379		:80	SYN_SENT	12s		0 B/s
123.153.63.63:47641		:80	SYN_SENT	9s		0 B/s
60.1.182.174:10837		:80	SYN_SENT	17s		0 B/s
183.253.21.227:21646		:80	SYN_SENT	12s		0 B/s
122.247.158.155:7359		:80	SYN_SENT	30s		0 B/s
101.66.89.143:43937		:80	SYN_SENT	30s		0 B/s
112.254.92.31:56869		:80	SYN_SENT	18s		0 B/s
101.24.181.39:8164		:80	SYN_SENT	15s		0 B/s
112.49.182.33:57205		:80	SYN_SENT	25s		0 B/s
117.45.253.120:53217		:80	SYN_SENT	9s		0 B/s
112.51.19.28:20134		:80	SYN_SENT	10s		0 B/s
TOTAL						0 B/s
Connections 1-21 of 2121			Unpaused	Unsorted		

Gambar 7. Serangan SYN Flood terhadap server Pustaka

Mekanisme terjadinya *SYN Flood* ini seperti dapat dilihat pada Gambar 6, memanfaatkan *TCP three way handshake*, dimana *threat actor* mengirimkan paket SYN ke server tanpa ada balasan sehingga membuat koneksi server menunggu balasan yang mengakibatkan user lain tertolak ketika akan melakukan akses ke server.

Serangan *SYN Flood* ini pernah dialami oleh server PUSTAKA. Penyerang mengirim ribuan paket SYN per detik sehingga server PUSTAKA menjadi penuh dan menyebabkan pengguna sah kesulitan akses terhadap aplikasi web yang terdapat pada server tersebut. Pada gambar 7 terdapat hasil tangkapan layar serangan *SYN Flood* ke server Pustaka.

Sampai saat ini berbagai ancaman yang terjadi pada infrastruktur TI masih dapat ditangani dengan baik oleh tim TI PUSTAKA dan tidak menyebabkan sesuatu yg dapat merusak data digital yang dimiliki. Guna mengoptimalisasi pelaksanaan pencegahan, penanggulangan dan pemulihan insiden, hasil monitoring aktivitas keamanan siber secara rutin dikoordinasikan dengan tim Kementan CSIRT (*Computer Security Incident Response Team*).

(Moh Afrillian Ramadhan, Boy Dewa Priambada, Rahman Sujatman)