DINAS KOMUNIKASI
DAN INFORMATIKA
KOTA MATARAM

FILELESS MALWARE

BISA BEROPERASI TANPA MENINGGALKAN JEJAK

Fileless malware tidak meninggalkan jejak di hard drive, sementara malware "biasanya" berjalan sepenuhnya di random-access memory (RAM) komputer.

DINAS KOMUNIKASI
DAN INFORMATIKA
KOTA MATARAM

BAGAIMANA MALWARE INI BISA MASUK ?

1. Melalui email phishing, malware masuk dan take over system utilities
2. Malware bersembunyi di program yang masuk whitelisted dengan hak sistem yang tinggi
3. PowerShell dan Windows Management Instrumentation (WMI) digunakan menjadi senjata
4. Malware langsung menjalankan payload di dalam memori, bukan di disk.
5. Malware ini menggunakan proses Windows yang valid sebagai host, dan kode yang ditambahkan berjalan sepenuhnya di RAM
6. Karena tidak ada file yang mencurigakan dengan teknik deteksi konvensional infeksi ini hampir sepenuhnya diabaikan.

@mataram.kita
fb.me/Pemerintah Kota Mataram
diskominfo.mataramkota.go.id

layanan.mataramkota.go.id

csirt.mataramkota.go.id

DINAS KOMUNIKASI
DAN INFORMATIKA
KOTA MATARAM

Dinas Komunikasi dan Informatika Kota Mataram membuka layanan aduan siber bagi masyarakat dan perangkat daerah yang menemukan atau mengalami kendala ataupun insiden terkait keamanan siber.

Terjadi Insiden Siber

Kumpulkan bukti insiden
(foto/screenshoot/log)
yang ditemukan

Tindak lanjut
oleh MATARAMKOTA-CSIRT

Kirim ke email : csirt@mataramkota.go.id
atau laman
https://helpdesk.mataramkota.go.id
(kategori Aduan Siber)

Proses verifikasi
oleh MATARAMKOTA-CSIRT

@mataram.kita
fb.me/Pemerintah Kota Mataram
diskominfo.mataramkota.go.id

layanan.mataramkota.go.id

csirt.mataramkota.go.id