Ver. 1.0.07062020_Bahasa_Indonesia

Enterprise Data Breach Prevention using MITRE ATT&CK Framework

Dalam kasus *cyber attack* dengan tujuan pencurian data (***data theft/exfiltration***), Tactics, Techniques, dan Procedures (TTPs) yang digunakan oleh Threat Actor dapat sangat kompleks dan bervariasi. Meskipun demikian, sebagian besar teknik-teknik tersebut telah berhasil diidentifikasi oleh MITRE dan dimasukkan dalam kategori **Exfiltration.** Berdasarkan MITRE ATT&CK Framework, **Exfiltration** adalah Tactic yang dilakukan oleh Threat Actor untuk mencuri dan mengirimkan data dari sistem yang sudah ter-*compromised* ke infrastruktur Command and Control (C&C) milik Threat Actor.

MITRE ATT&CK Enterprise Tactics

Initial Access → Execution → Persistence → Privilege Escalation → Defense Evasion → Credential Access → Discovery → Lateral Movement → Collection → Command & Control → **Exfiltration** → Impact

MITRE ATT&CK Exfiltration Techniques

T1002 Data Compressed
Pencurian data dengan melakukan kompresi data untuk memperkecil ukuran data yang akan dicuri/dikirimkan serta untuk menghindari deteksi. Umumnya menggunakan compression library seperti 7zip, RAR, ZIP, atau zlib.

T1022 Data Encrypted
Pencurian data dengan melakukan enkripsi data untuk menyembunyikan informasi sensitif pada data yang akan dicuri/dikirimkan. Menghindari deteksi secara statis (menggunakan signature) dan mempersulit proses forensik serta investigasi.

T1020 Automated Exfiltration
Pencurian data menggunakan teknik scripting secara otomatis dengan logika pemograman. Biasanya digunakan secara bersamaan dengan teknik Exfiltration lainnya, misalnya: pencurian data dengan file extensions tertentu setiap 60 menit ke C&C server.

T1030 Data Transfer Size Limits
Pengiriman data dengan ukuran yang kecil dan fixed size, daripada mengirimkan keseluruhan data yang besar secara bersamaan dan terus-menerus. Dilakukan untuk menghindari deteksi terhadap pengiriman data yang melebihi batas wajar (threshold).

T1048 Exfiltration Over Alternate Protocol
Pencurian data melalui protokol yang tidak umumnya digunakan dan/atau berbeda dari protocol C&C, misalnya melalui DNS, SMTP, FTP, ICMP, SMB dan HTTP/S. Misalnya DNS Tunneling dan ICMP Tunneling, untuk menghindari penerapan deteksi yang terbatas pada protokol tertentu.

T1041 Exfiltration Over Command & Control Channel
Pencurian data dengan mengirimkan data melalui Command & Control (C&C) Channel, yaitu channel yang sebelumnya digunakan oleh Threat Actor untuk beroperasi dan melakukan eksekusi command pada target secara remote dari jaringan eksternal.

T1011 Exfiltration Over Other Network Medium
Pengiriman data melalui konektivitas lain selain default connection, misalnya Bluetooth, RF Channel, Modem, WiFi Connection, dan Cellular Data untuk menghindari deteksi karena konektivitas lain tersebut tidak termonitor dan diproteksi secara memadai.

T1052 Exfiltration Over Physical Medium
Pencurian data melalui perangkat penyimpanan fisik seperti USB FlashDisk, External HardDisk Drive, MP3 Player, Smartphone dan media penyimpanan fisik lainnya.

T1029 Scheduled Transfer
Mengirimkan data secara terjadwal pada waktu atau pola interval tertentu untuk menghindari deteksi dan agar menyerupai (blend-in) dengan aktivitas normal.

T1537 Transfer Data to Cloud Account
Mengirimkan atau melakukan backup data yang ditujukan ke Account lain milik Threat Actor, namun masih di dalam cloud provider yang sama untuk menghindari deteksi.

Know Your Enemy

Recommended Mitigations Techniques

Implement:
1. **Network Proxy** untuk seluruh jaringan dan terapkan kebijakan yang ketat untuk penggunaanya tanpa terkecuali
2. **Network Traffic Filter** untuk mencegah/memblokir koneksi jaringan selain melalui protokol, port, atau IP Address yang sudah ditentukan dan disepakati (whitelist)
3. **Network Segmentation** terhadap critical infrastructure dengan hanya memperbolehkan koneksi masuk/keluar melalui protokol, port, atau IP address yang sudah ditentukan dan disepakati (whitelist)
4. **Network Intrusion Prevention** untuk dapat mencegah/memblokir traffic yang ditujukan ke Infrastruktur C&C dengan menggunakan signature berdasarkan IP Address, Negara, ASN atau signature lainnya yang terindikasi malicious. (blacklist)
5. **Data Loss Prevention (DLP)** untuk mencegah pengiriman terhadap suatu jenis file dengan extension, nama file, atau keyword tertentu. (blacklist)
6. **Dedicated Server** untuk suatu internal network services (misalnya dedicated internal DNS server) dan hanya memperbolehkan koneksi ke server tersebut melalui port/protokol secara spesifik.
7. Konfigurasi pada sistem operasi untuk **mencegah pembuatan network adapter baru**, **menonaktifkan Autorun**, **menonaktifkan/mencegah penggunaan media penyimpanan fisik** sesuai kebijakan perusahaan
8. **Network Filter Traffic** untuk mencegah adanya pengiriman data ke Cloud Server/Instance lain selain yang telah ditentukan, meskipun masih dalam Cloud Provider yang sama.
9. Konfigurasi password dan hak akses berdasarkan prinsip **least privileges**. Password rotation dan expiry pada periode waktu tertentu untuk mencegah penggunaan User Credentials yang **pernah** dicuri atau breached.

Prevention Strategies

Monitor:
1. **Eksekusi process dan command** yang terkait dengan **compression utilities** seperti seperti Tar.gz, 7zip, RAR, ZIP, atau zlib..
2. **Eksekusi process dan command** yang terkait dengan **encryption utilities**. Misalnya memonitor terhadap process-process yang memanggil Windows DLL 'crypt32.dll'
3. **Monitoring** (pada jaringan maupun endpoint) terhadap pola (pattern) dan adanya kondisi-kondisi **anomali** yang tidak sesuai dengan kondisi normal. Misalnya, adanya client/endpoint yang secara tiba-tiba mengirimkan data dalam jumlah besar dengan protocol atau tujuan yang tidak biasanya, adanya koneksi pengiriman data ke suatu tujuan secara terus-menerus atau pada waktu-waktu tertentu. Dan lain sebagainya sesuai dengan kondisi normal suatu sistem dan infrastruktur
4. **Aktivitas pengiriman data** melalui jaringan pada protokol-protokol yang tidak biasa digunakan (uncommon) untuk mendeteksi adanya **tunneling** untuk eksfiltrasi data.
5. **Aktivitas pengiriman data, snapshot, backup data** dengan menggunakan atau dengan ditujukan ke Cloud Account yang tidak semestinya digunakan atau untrusted.
6. **Penambahan atau perubahan terhadap konfigurasi network interfaces/adapter** pada sistem operasi.
7. **Akses file ke media penyimpanan fisik** dan deteksi adanya eksekusi process ketika media penyimpanan terpasang atau mounted pada sistem operasi.

Detection Strategies

Win The Battle

Disclaimer
Mitigasi di atas bersifat umum dan minimum. Pada implementasinya harus disesuaikan dan diperkuat sesuai kondisi pada infrastruktur perusahaan masing-masing. Penjelasan lebih lengkap dapat dilihat pada: https://attack.mitre.org/tactics/TA0010/

Penyusun: Ade Firman Triangga (linkedin.com/in/ade-firman-triangga/)
Reviewer: Cyber Defense Indonesia Community

"Turut Mencerdaskan Bangsa Melalui Tulisan dan Pemikiran"

Komunitas Cyber Defense Indonesia – https://cdef.id/