

# SIGHTINGS ECOSYSTEM

A DATA-DRIVEN ANALYSIS OF ATT&CK IN THE WILD

Received 6m+ Sightings, pared down to 1.1m after normalizing data, across 184 unique techniques observed between April 2019 and July 2021.

2019 - 2021  
APRIL JULY

**6M+**

SIGHTINGS

**1.1M**

NORMALIZED  
SIGHTINGS

**184**

UNIQUE  
TECHNIQUES

## COMMON ADVERSARY BEHAVIORS



Which techniques  
adversaries use



How their use  
changes over time



How adversaries use  
techniques together

# 15 TECHNIQUES

made up 90% of the observed techniques from April 2019 - July 2021. Most of these techniques abuse legitimate system tools.

Command and Scripting  
Interpreter [T1059]

Scheduled Task/Job [T1053]

Proxy [T1090]

Hijack Execution Flow [T1574]

Masquerading [T1036]

Non-Application Layer  
Protocol [T1095]

Create or Modify  
System Process [T1543]

Signed Binary/Proxy  
Execution [T1218]

Impair Defenses [T1562]

Process Injection [T1055]

Obfuscated Files or  
Information [T1027]

Windows Management  
Instrumentation [T1047]

Remote Services [T1021]

Modify Registry [T1112]

Ingress Tool Transfer [T1105]

# 10 NIST 800-53 CONTROLS

---

provide the coverage for the most observed techniques

- 1** SI-4 System Monitoring
- 2** CM-6 Configuration Settings
- 3** CM-2 Baseline Configuration
- 4** CM-7 Least Functionality
- 5** AC-3 Access Enforcement
- 6** AC-6 Least Privilege
- 7** AC-2 Account Management
- 8** AC-5 Separation of Duties
- 9** CM-5 Access Restrictions for Change
- 10** IA-2 Identification and Authentication (Organizational Users)