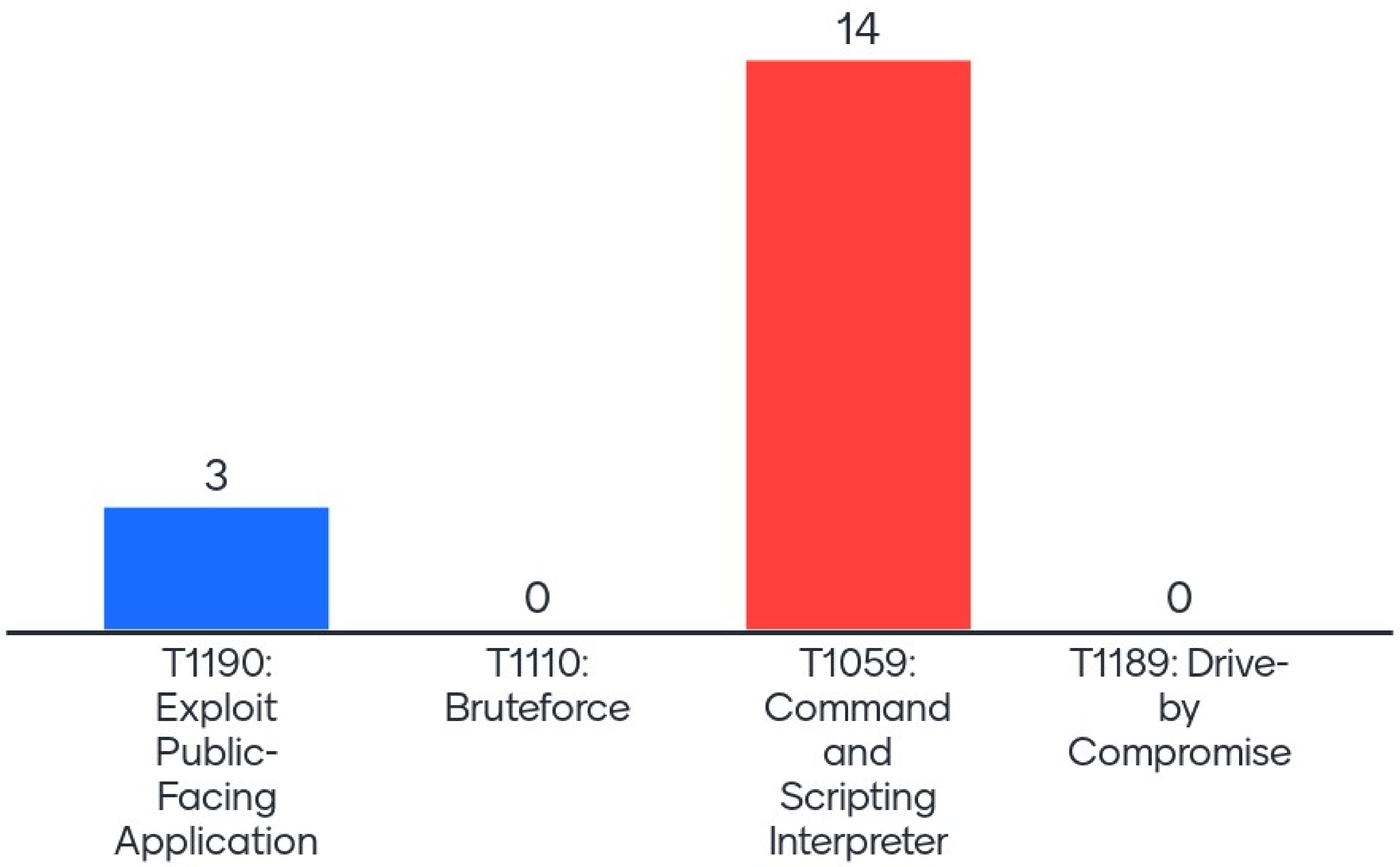
TTP Mapping

9

Mentimeter

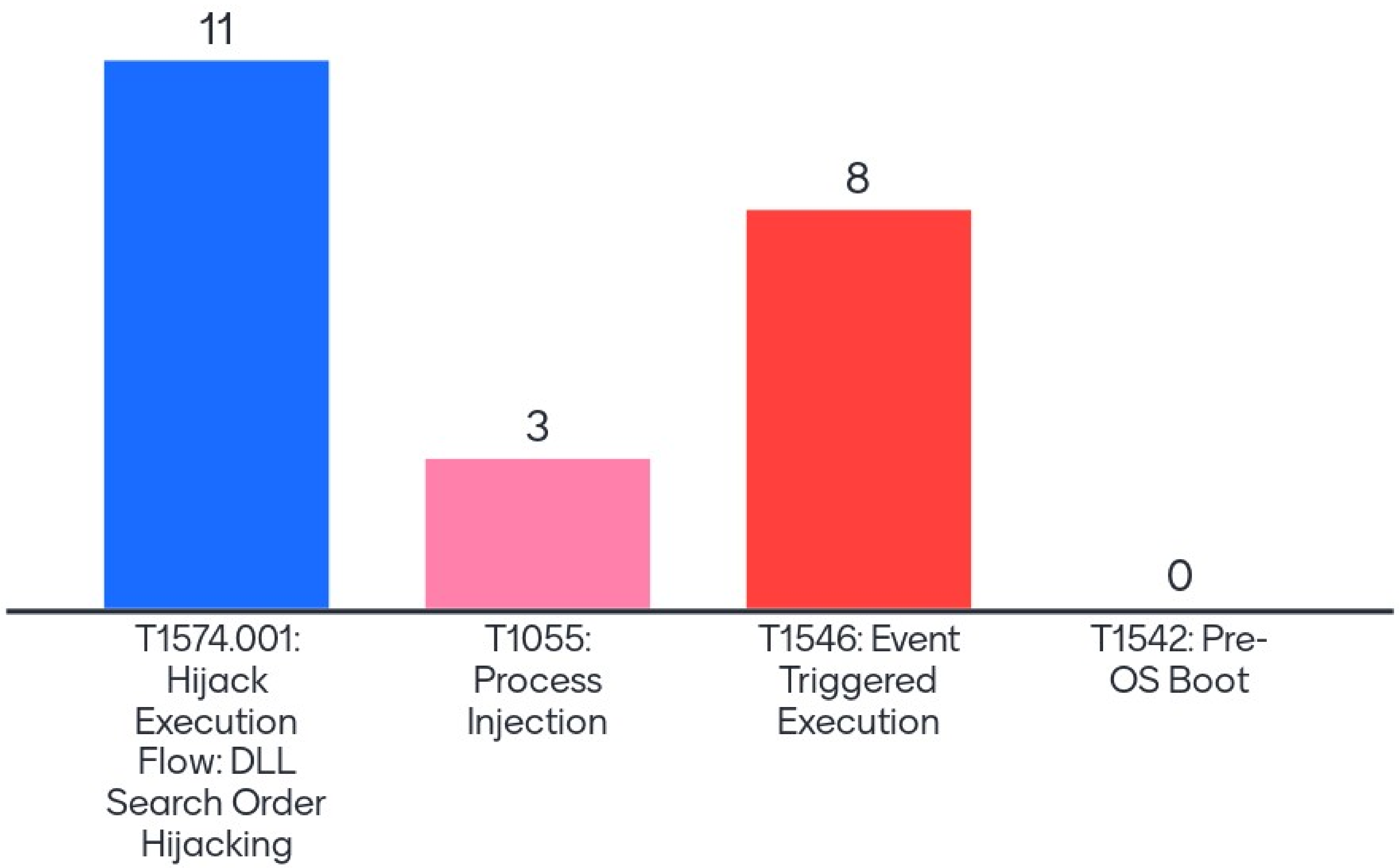
The group has used SQL injection for initial compromise



10 👍 17 👤

Mentimeter

The group has used search order hijacking to force TeamViewer to load a malicious DLL

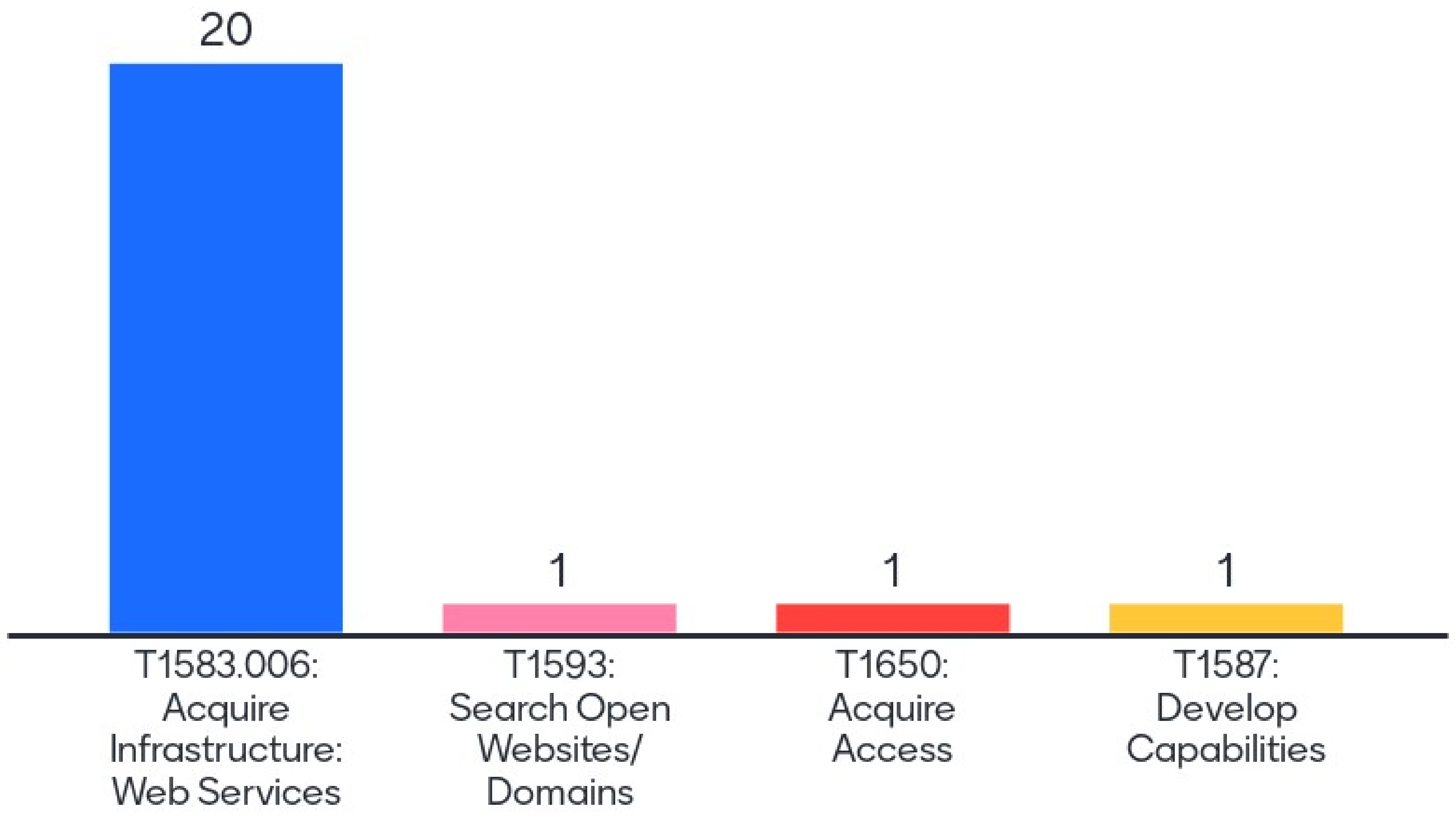


9

22

Mentimeter

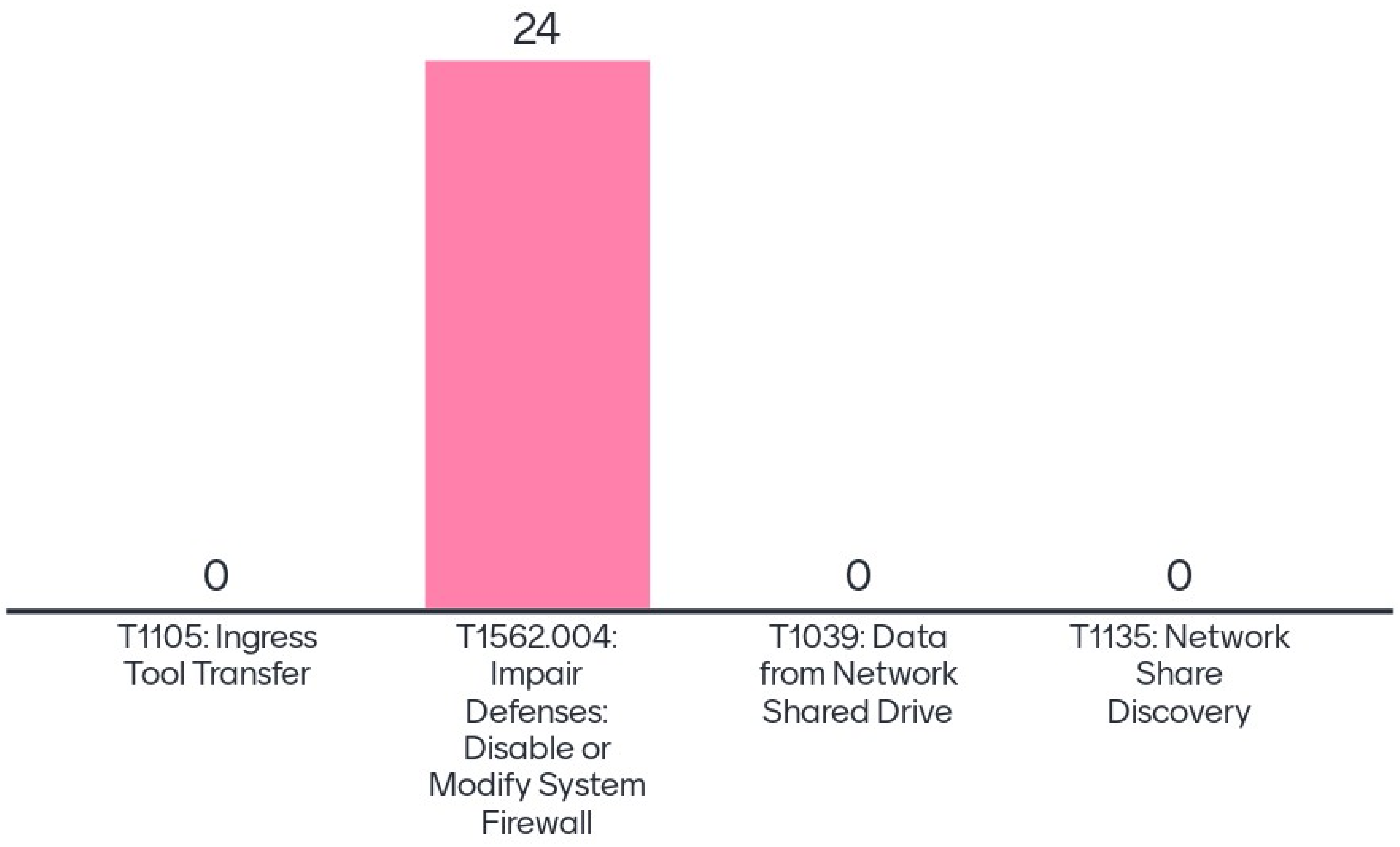
Lazarus Group has acquired domains related to their campaigns to act as distribution points and C2 channels



11

23

The malware modifies the Windows firewall to allow incoming connections or disable it entirely

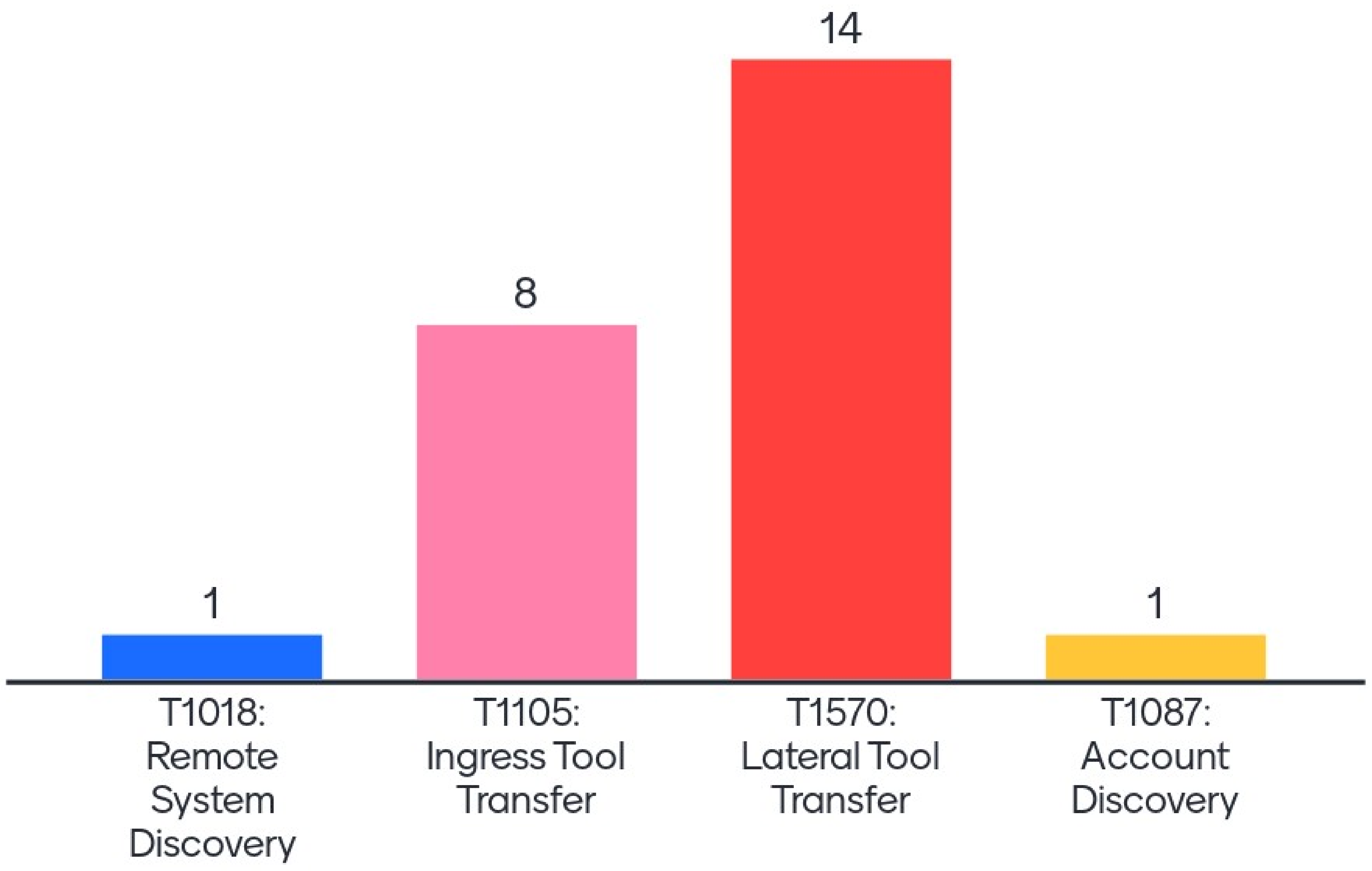


9

24

Mentimeter

Magic Hound has copied tools within a compromised network using RDP

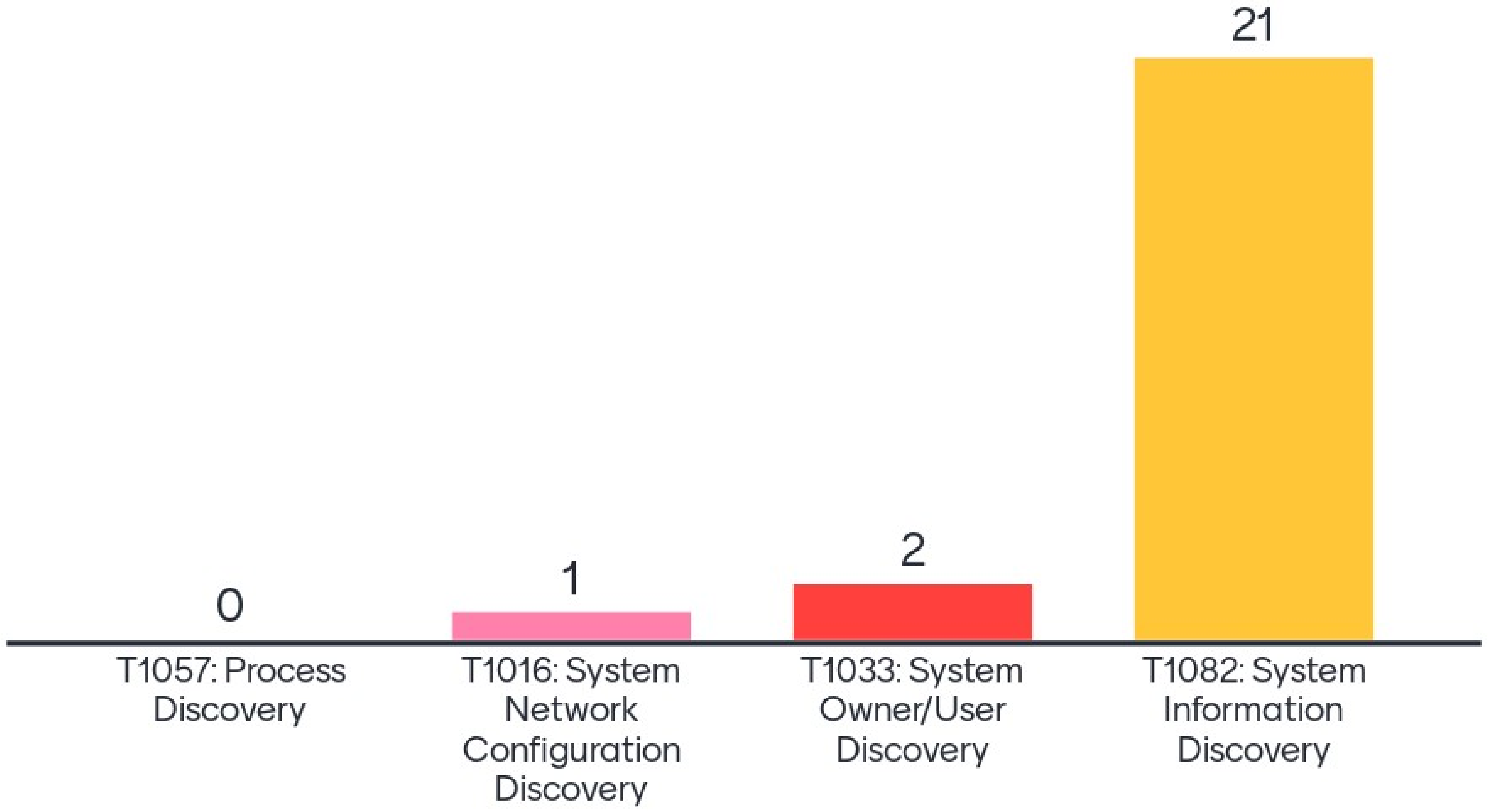


11

24

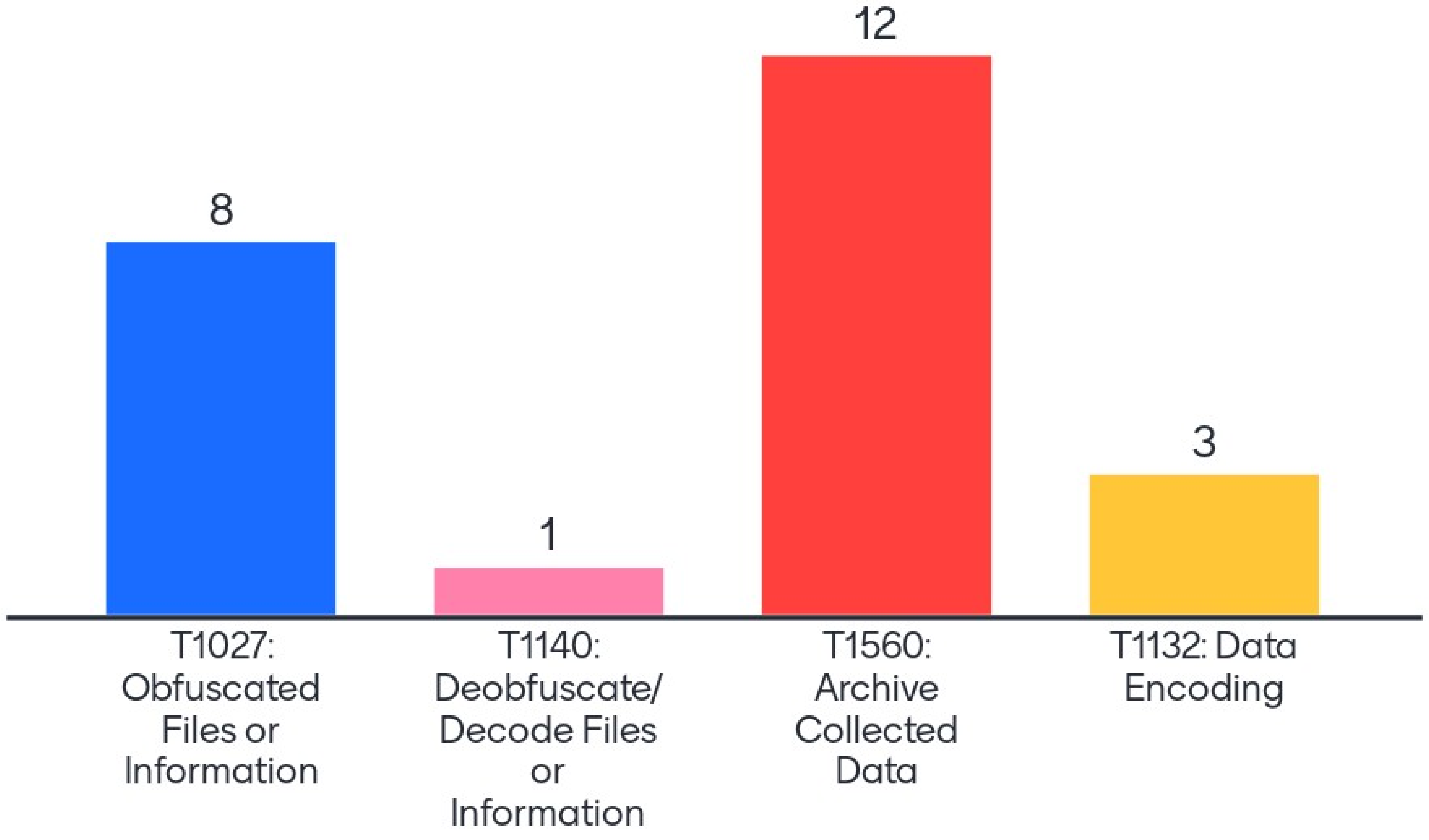
Mentimeter

The malware has collected the computer name and OS version from a compromised machine



Mentimeter

menuPass has compressed files before exfiltration using TAR and RAR.

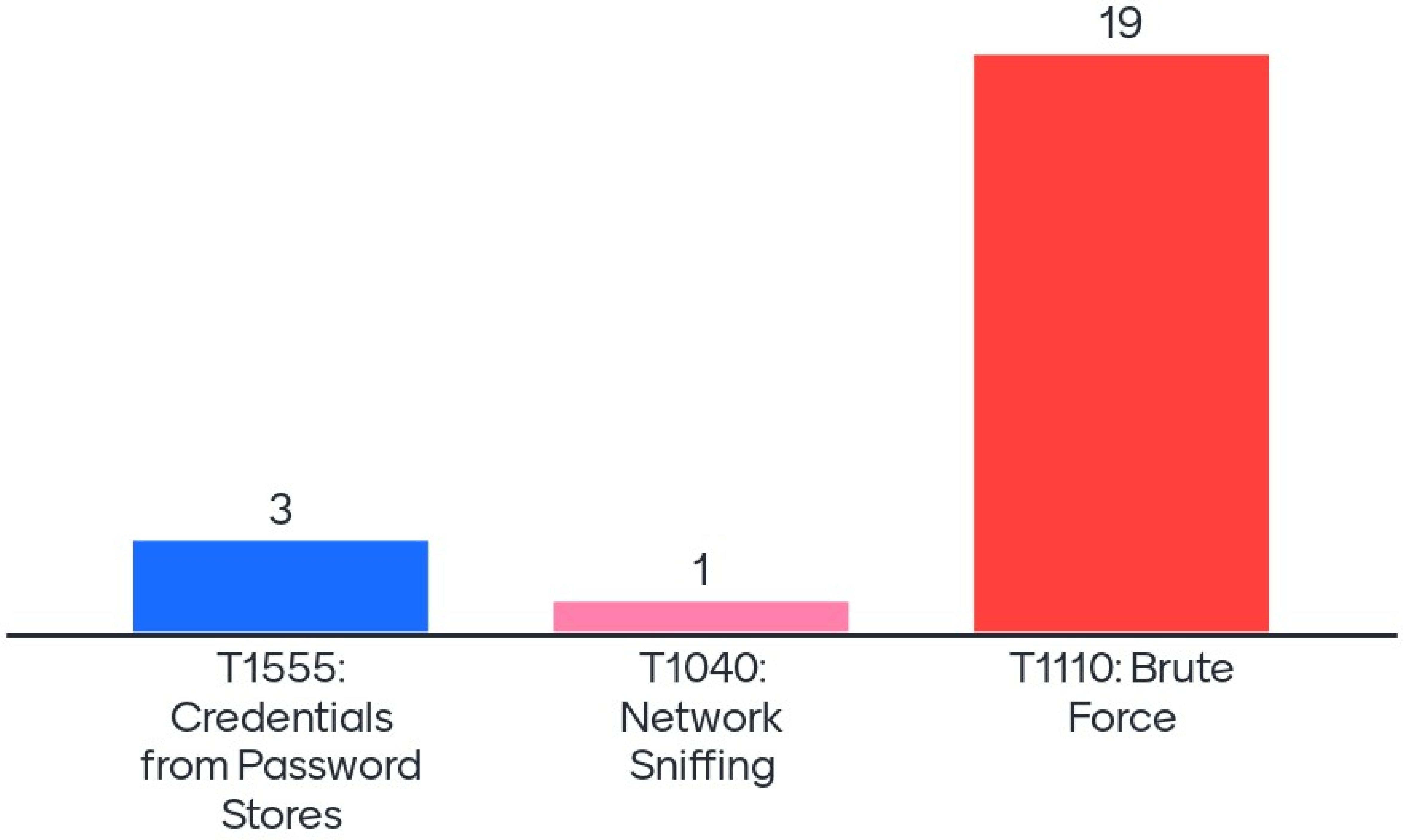


7

24

Mentimeter

OilRig has used brute force techniques to obtain credentials

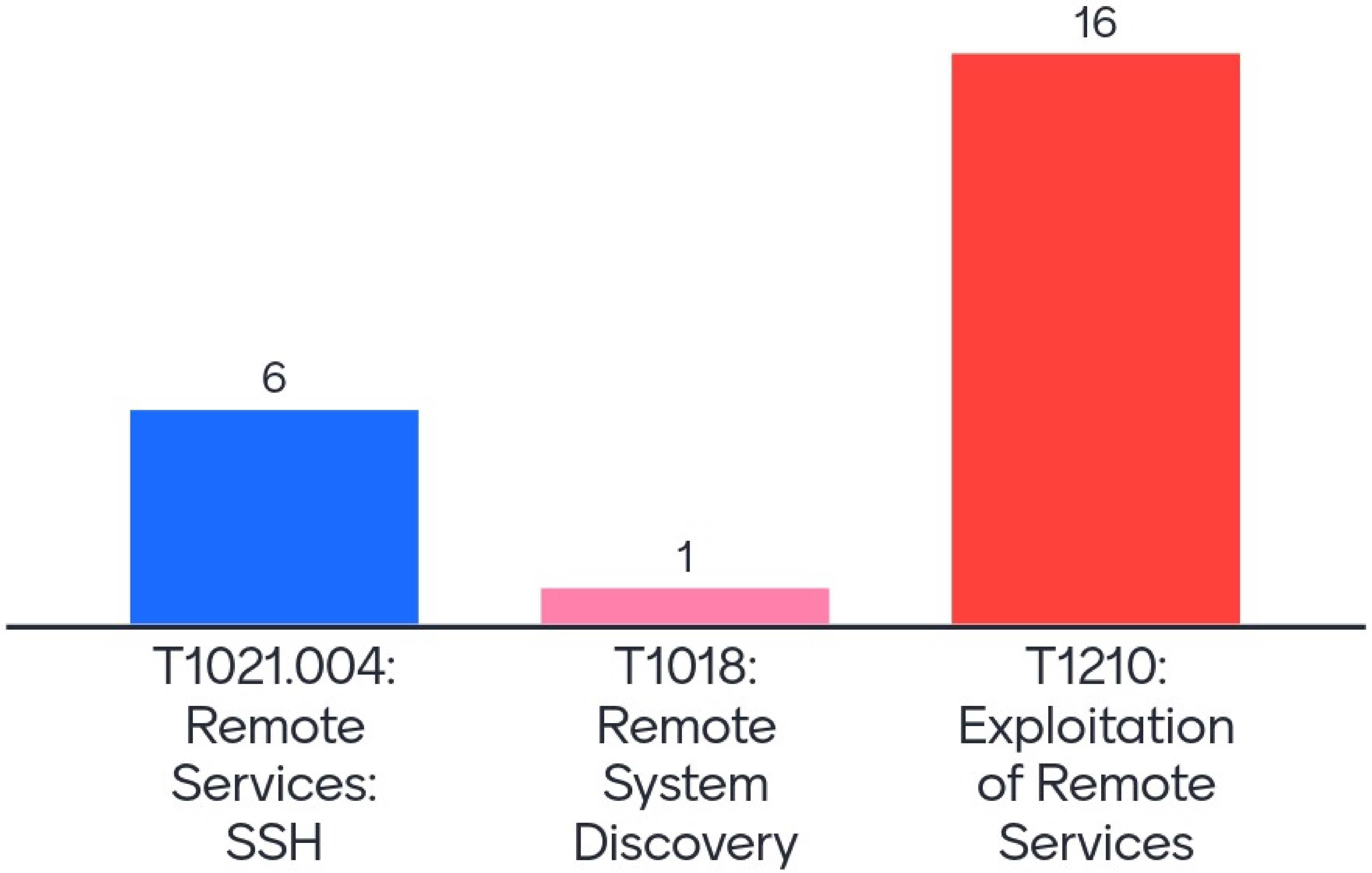


12

23

Mentimeter

OilRig has used Putty to access compromised systems

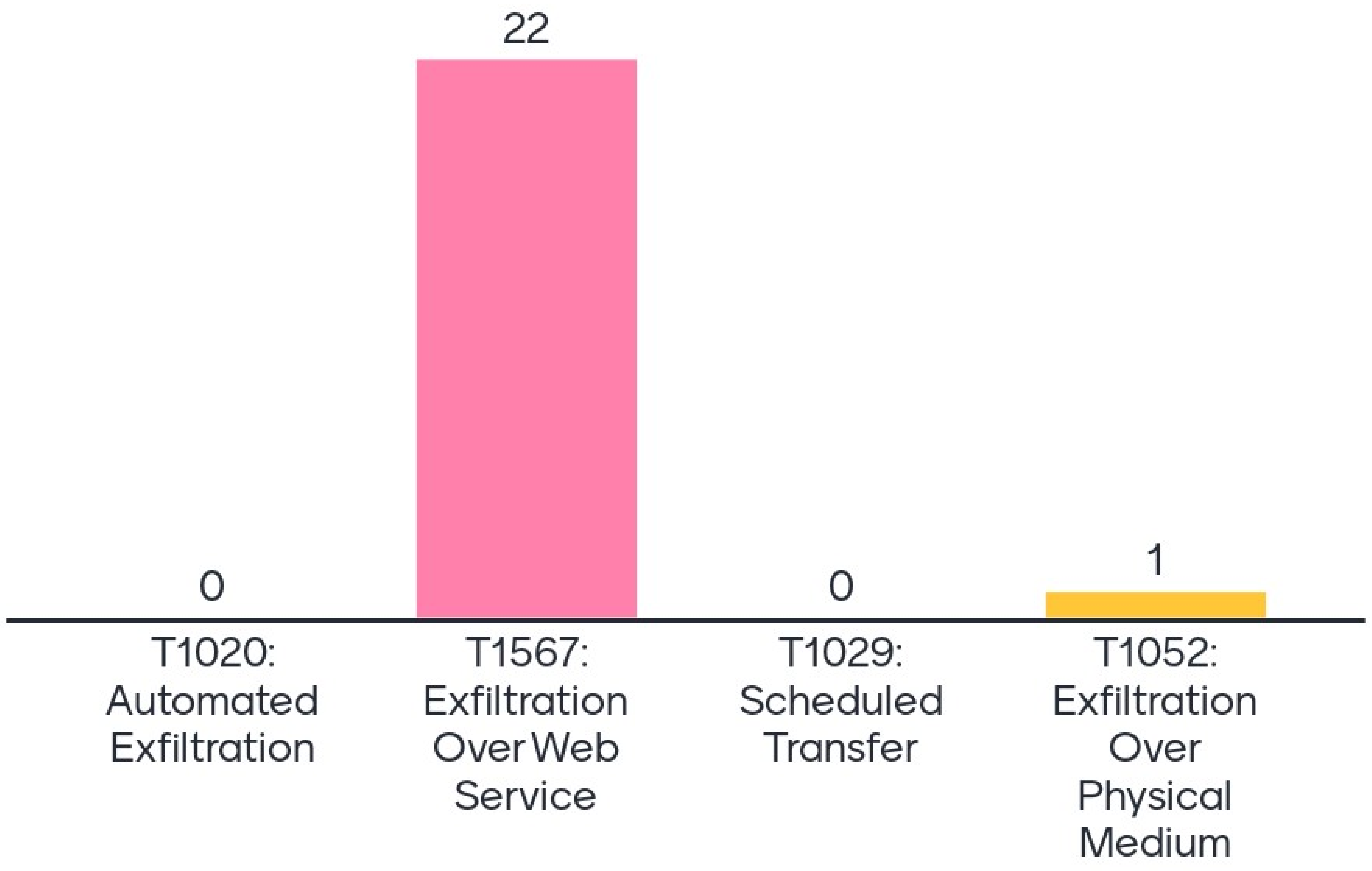


9

23

Mentimeter

Turla has exfiltrated stolen files to OneDrive and 4shared



2

23