

THE RED REPORT 2023

Key Findings

#1 Lateral Movement: Evolution of Attack Techniques

Attackers use techniques such as *Remote Services*, *Remote System Discovery*, and *WMI* for Lateral Movement, allowing them to pivot from a compromised system deep into the victim's network.



#2 Ransomware: Data Encryption Remains a Top Threat

Data Encrypted for Impact remains the third most used technique by adversaries. Found in almost a quarter of all malware analyzed, it highlights ransomware's threat to organizations.



#3 Remote Discovery and Access: Abusing Built-in Tools

Attackers abuse built-in tools and protocols like RDP, SSH, net, and ping to remotely access systems, showing a preference for remote access tactics in moving laterally undetected.



#4 Credential Dumping: Outsmarting Traditional Perimeter Security

Traditional perimeter security is no longer enough to protect against cyberattacks. Prioritizing cyber resilience to defend against pre and post-compromise attacks is critical.



#5 Stealthy Attacks: Weaponizing Legitimate Software

To execute arbitrary commands and discover system information, attackers use native tools such as PowerShell, which include utilities for *Credential Dumping*, *Remote Services*, and *Scheduled Task/Job*.



#6 Malware Evolution: Rise of Multi-faceted Tactics

While malware leverages 10 TTPs, more than a third of analyzed malware can exhibit more than 20 TTPs, and one-tenth uses over 30 TTPs. This indicates highly sophisticated tactics.



Want to learn more about the ATT&CK techniques and emerging threats that dominate the cybersecurity landscape?

[READ FULL REPORT](#)