The Enterprise is the Number One Target for Nation States

- Enterprises: 35%
- Cyberterrorism: 15%
- Media and communication outlets: 14%
- Government bodies or regulators: 12%
- Critical infrastructure: 10%
- Other: 8%

Endpoints Are the First Line of Defense – Protect Them

- Refocus Protection: Endpoints are the number one point of infection, defend them.
- Stay Ahead of Threats: Adopt endpoint security architecture built on Zero Trust principles.
- Secure-by-design: Resilience should start at hardware level, then extend across software and services.
- Reinforce your endpoints: Harden defenses to contain threats and recover from cyberattacks.

Nation State CyberWeapons Vary in Sophistication and Scope

- 50% of cyberattacks involved low-budget tools.
- 20% of cyberattacks involved custom-made malware or weaponized exploits.

Most Common Applications for CyberWeapons are:

- Surveillance: 50%
- Network Incursion and Positioning: 15%
- Damage or Destruction: 14%
- Data Exfiltration: 8%

© Copyright 2021 HP Development Company, L.P. ABOUT THE RESEARCH

Nation States, CyberConflict and the Web of Profit is an academic study that was originally launched by Bromium in April of 2018—Bromium was acquired by HP in September 2019. The report is sponsored by HP, and researched and written by Dr. Mike McGuire, Senior Lecturer in Criminology at the University of Surrey. Nation States, CyberConflict and the Web of Profit is the fourth installment in the Web of Profit body of research. The findings contained in this report are the culmination of an analysis of known Nation State cyberattacks up to February 2021, alongside interviews with an expert panel of leading practitioners.