Subgroup: Longhorn, The Lamberts - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 01:02:49 UTC

DescriptionA subgroup of the CIA.

Some operations and tooling used by this group were exposed in the [Vault 7/8] leaks on WikiLeaks in 2017.

(Symantec) Longhorn has been active since at least 2011. It has used a range of back door Trojans in addition to zero-day vulnerabilities to compromise its targets. Longhorn has infiltrated governments and internationally operating organizations, in addition to targets in the financial, telecoms, energy, aerospace, information technology, education, and natural resources sectors. All of the organizations targeted would be of interest to a nation-state attacker.

Longhorn has infected 40 targets in at least 16 countries across the Middle East, Europe, Asia, and Africa. On one occasion a computer in the United States was compromised but, following infection, an uninstaller was launched within hours, which may indicate this victim was infected unintentionally.

Longhorn’s malware appears to be specifically built for espionage-type operations, with detailed system fingerprinting, discovery, and exfiltration capabilities. The malware uses a high degree of operational security, communicating externally at only select times, with upload limits on exfiltrated data, and randomization of communication intervals—all attempts to stay under the radar during intrusions.

For C&C servers, Longhorn typically configures a specific domain and IP address combination per target. The domains appear to be registered by the attackers; however they use privacy services to hide their real identity. The IP addresses are typically owned by legitimate companies offering virtual private server (VPS) or webhosting services. The malware communicates with C&C servers over HTTPS using a custom underlying cryptographic protocol to protect communications from identification.
