TLP WHITE:
Executive Threat Intelligence Briefing on Earth Kapre/RedCurl

Overview
Earth Kapre, also known as RedCurl, is a notable threat actor engaged in sophisticated cyber espionage since at least November 2018. Their primary focus is on infiltrating corporations across various sectors worldwide to steal sensitive documents and data. This briefing outlines their methods, targets, and the implications for our corporate security posture.

Operational Profile
Scope of Operations: Earth Kapre's espionage campaigns are global, with documented activities in countries including the U.K., Germany, Canada, Norway, Russia, and Ukraine. Their targets span multiple industries, emphasizing the diversity and breadth of their operations.
Methodology: Unlike typical cybercriminals, Earth Kapre employs a mix of custom-developed malware and publicly available hacking tools. They focus on stealth and the strategic use of technology to infiltrate networks, avoiding detection while extracting valuable corporate data. Their operations can last anywhere from two to six months within a compromised network.

Risks and Implications
Data Theft: The group's primary goal is the theft of internal corporate documents, which can include everything from staff records and legal documents to sensitive strategic plans. This poses a direct threat to the integrity and confidentiality of our corporate data.
Sophistication and Stealth: Earth Kapre's ability to bypass traditional security measures and remain undetected for extended periods highlights the need for advanced threat detection and response strategies within our security posture.

Key Indicators of Compromise (IoCs)
Malicious Domains/IPs: The group has been associated with specific domains and IP addresses used for malicious activities. Monitoring network traffic for connections to these indicators can aid in early detection.

Malware Signatures: While specific malware file hashes were not detailed in this summary, vigilance against files downloaded from suspicious sources remains crucial.
Anomalous Network Activity: Unusual network patterns, such as out-of-hours connections or unexpected data flows to external IPs, should be investigated promptly.

Defensive Strategies
Enhanced Monitoring: Implement advanced network monitoring tools to detect and alert on suspicious activity associated with the group's known IoCs.

Incident Response Plan: Ensure that an up-to-date incident response plan is in place, specifically tailored to address the types of threats posed by groups like Earth Kapre.
Education and Awareness: Increase awareness of phishing and other social engineering tactics among staff to prevent initial breaches.

Conclusion

Earth Kapre/RedCurl's activities underscore the evolving landscape of cyber threats facing corporations today. Their focus on stealthy data exfiltration and the use of sophisticated tools and techniques highlight the necessity for a proactive and dynamic approach to cybersecurity within our organization. By enhancing our detection capabilities and fostering a culture of security awareness, we can better protect our assets against such advanced persistent threats.