Phishing: The Gateway to Compromise

AT A GLANCE

- **Top Targeted Industries:** Phishing attacks are heavily concentrated in sectors handling sensitive data and financial transactions, including **Banking & Finance (17%)**, **Manufacturing (13%)**, **Business Services (11%)**, **Construction (9%)**, and **Healthcare (9%)**.
- **The Human Factor is the Target:** Phishing is a social engineering attack that exploits human psychology using urgency, fear, and trust to trick employees into clicking malicious links or opening dangerous attachments.
- **The 9-to-5 Attack Window:** Threat actors are strategic, launching the majority of phishing campaigns on **Tuesdays (23%)** and timing them between **1600 and 1900 UTC** to coincide with North American business hours when employees are most active and potentially distracted.
- **The Initial Access King:** Phishing (MITRE ATT&CK® T1566) is the dominant initial access vector, accounting for over **78%** of related alerts and serving as the starting point for more severe attacks like ransomware and data breaches.

OVERVIEW

Phishing is more than just spam; it is the most prolific and effective method for gaining initial access to a corporate network. By masquerading as trusted entities, malicious actors manipulate employees into divulging sensitive information, from login credentials to financial data. Unlike technically complex exploits, phishing attacks target the most unpredictable vulnerability in any organization: its people.

Our latest analysis of security alerts reveals a calculated approach by threat actors. They are overwhelmingly targeting industries where a successful credential compromise can lead to immediate financial gain or access to valuable intellectual property. **Banking & Finance** leads as the top target at 17%, followed closely by **Manufacturing** at 13%.

Modern phishing campaigns are highly sophisticated. Attackers conduct thorough reconnaissance to craft convincing lures, impersonating executives, IT support, or trusted business partners. These attacks are timed to perfection, hitting inboxes during the busiest parts of the workday when employees are most likely to let their guard down. Once a user clicks a malicious link or opens a compromised attachment, the gateway is open for attackers to steal data, deploy ransomware, or establish a long-term foothold in the network.

This report contains valuable insights and recommendations for defending against modern phishing attacks. To unlock the full content, reach out to your customer success manager or email info@criticalstart.com.

Critical Start comprehensive MDR provides coverage across your Microsoft environment and beyond. Their 24x7x365, U.S.-based Security Operations Centers (**SOC**s) provide AI-accelerated, human-validated detection and response that ensures escalations represent true positives. You'll also have the power to triage and contain threats on-the-go with their full-featured MOBILE**SOC**® mobile app. With contractual SLAs for threat alerts and full SOC transparency — including contextualized justification for every alert closure, regardless of criticality — you will know exactly what is happening within your environment so you can stay ahead of threats.