Article

Mar 2026

The art of deception: How honeypots strengthen network defences

Detecting cyber criminals within a complex network can be difficult. Internal threats that have breached the perimeter can operate under the radar for extended periods. Once inside, attackers may mimic legitimate users, exploit systems, and move throughout the network without raising suspicion.

Traditional security tools like firewalls and antivirus software are not always compatible with the various technologies businesses employ, meaning attackers may exploit systems that aren't covered by effective detection controls. The rise of IoT, embedded devices, BYOD and even shadow IT can amplify this - introducing blind spots to an organisations threat detection strategy.

Additionally, advanced logging and monitoring tools may collect vast amounts of data, but without context or behavioural analysis, anomalies can go unnoticed. The sheer volume of network traffic and user activity creates a noisy environment where subtle signs of intrusion are easily lost. Having holistic internal network traffic inspection/IPS coverage, or SIEM solutions with complex detection capabilities, can also be expensive and difficult to deploy.

The consequences of undetected cyber criminals operating within an internal network can be devastating. Once inside, attackers can exfiltrate sensitive data, disrupt operations, and even deploy ransomware. Intellectual property, customer information, financial records, and strategic plans are all at risk. The longer an attacker remains undetected, the more damage they can inflict.

To counter these threats, organisations are increasingly deploying honeypots and honey tokens, which are deceptive security mechanisms designed to lure and detect malicious actors. A honeypot is a decoy system or service that appears legitimate but is isolated and monitored. It might mimic a database, file server, or login portal. When an attacker interacts with it, security teams are alerted to suspicious activity that would otherwise go unnoticed.

Honey tokens, on the other hand, are fake credentials, files, or data elements planted within the network. These tokens are designed to be enticing to attackers, such as a document labelled "Payroll_2025.xlsx" or a set of credentials embedded in a config file. Any attempt to access or use these tokens triggers an alert, revealing the presence of an intruder.

Together, honeypots and honey tokens provide early warning systems that complement traditional defences. They don't just detect attacks, they reveal intent. Because legitimate users have no reason to interact with these decoys, any engagement is a strong indicator of malicious behaviour. This allows security teams to respond swiftly, isolate threats, and investigate further.

There are a myriad of both commercial and open-source honey pot and honey token solutions available. Some may even be built in to an organisations existing licensing, such as in Microsoft Defender for Identity. A popular free solution is OpenCanary due to being well documented, low-resource and its ability to mimic a broad list of network services. There are also commercial offerings too, with a Thinkst Canary being the paid-for version of OpenCanary, as well as SecurityHive being another popular, both of which have excellent honey token capabilities.

By turning the tables on attackers, these tools transform internal networks from passive targets into active traps, making it far riskier for cyber criminals to operate undetected