illusive

Financial Industry Under Attack

What do attackers want?

Attackers view financial institutions as gold mines. That is why the financial sector frequently suffers from the most advanced attacks.

In constant search of a new source of income, cybercriminals covet the unlimited access to global financial systems held by financial institutions, including access to financial transaction systems and trading systems. Furthermore, financial networks store an abundance of sensitive financial information. Potential profit from selling this valuable information on the dark web motivates attackers to target these networks.

Identified in 2015, the Carbanak APT was one of the largest modern bank robberies, hitting 100 banks and stealing 1 billion dollars.

What is the risk?

Cyber attacks don't just cause substantial fiscal damage; they can ruin the targeted organization. Financial institutions, especially banks, operate in an ecosystem based on mutual trust. To gain customer confidence, the financial sector invests heavily in promoting the perception that it can protect customer funds and financial data.

The credibility and perceived competence that customers give an institution can be severely damaged by the mere fact that an attacker gained access to the network, shaking the very foundations of the business relationship.

How does the attack operate?

Financial industry networks generally consist of many distributed hosts, plenty of non-technical users, and numerous sensitive assets. Attackers use targeted attacks (such as spear-phishing campaigns) to penetrate network defenses, and use lateral movements to diligently seek hosts with access to financial systems or sensitive information.

What are the challenges to protection?

- Growing demand for global accessibility of digitized financial services results in exponential growth of the attack surface.
- The legacy systems and old IT infrastructures in use can be easily compromised, once reached.
- Attackers are continuously becoming more sophisticated, designing attack tools specifically for financial systems.

What would minimize the risk?

As persistent attackers will always find a way onto your network, risks are minimized by detecting attacker presence before sensitive data is reached, feeding attackers false information, and blocking ransomware processes from real data.

With illusive's agentless solution installed, you can remediate the risk of using legacy systems without high cost infrastructure projects. The Deceptions Everywhere® solution deploys a layer of decoy data on every endpoint, server, and attack surface – that appear identical to what the attacker is seeing to fuel lateral movement. Once the decoy data is triggered, a high fidelity alert is generated and sensitive data remains intact. The Advanced Ransomware Guard™ deception family specifically blocks ransomware processes. To gain better optics into your network, illusive networks Attacker View™ offers visibility into large networks and identifies discoverable attack-vectors.