# Illusive Uses Deception to Reduce Cyber Risks for Financial Services


## Abstract

Over the last several months, deception technology provider Illusive Networks increased its focus on serving the financial services sector, adding a new API to provide security teams with a broader view of forensics data, new advanced persistent threat (APT) risk visibility features, and a specific Society for Worldwide Interbank Financial Telecommunications (SWIFT) module to better protect those using the money transfer network.



## Event

Illusive Networks, an Israeli deception technology startup, is expanding its capabilities in defending the financial services industry to help organizations better protect their "crown jewels" from cyber thieves. In late July 2017, Illusive introduced a new external incident application program interface, as well as some risk metric tools designed to help prioritize and streamline incident response and enable continual improvement of defenses against APTs. Developed at the request of financial services customers' security operations centers (SOCs), these tools enable alerts and data to be shared with other detection and protection products to deliver forensics data from compromised hosts. The API enables bidirectional information sharing between the Illusive solution and other security tools, such as SIEMs.

In Q4 2016, Illusive introduced a new deception option for its core suite that is dedicated to helping organizations better protect themselves against attacks aimed at SWIFT participants. This add-on, Wire Transfer Guard, contains a series of deceptions including decoys designed to look like objects that attackers can use to move toward elements of a wire transfer network, such as gateways, access servers, databases, credentials, and more. When an attacker tries to connect to a decoy, an alert is sent to security teams so they can mitigate the threat. Wire Transfer Guard also provides real-time, source-based forensics to help SOC operators and other incident responders dissect the attacker's campaign. Using the AttackerView feature of the interface, security analysts can visualize the potential attack paths between endpoints and risk-sensitive assets. Such assets can include customer-selected systems that contain valuable data or support business-critical processes, as well as systems that provide access to domain administrator credentials. With that perspective, operators can understand an attacker's ability to move laterally and see where their network is exposed so they can bolster its protection with more effective deception policies. The interface also provides a view into the movements of actual attackers based on data gathered from the compromised host, allowing operators to assess how close they are to the organization's most sensitive information, and then take steps to prevent access. The core solution's Deception Management System (DMS) learns how each customer's network is configured, including naming conventions for users, systems, and applications, and it learns communication patterns. Based on what it identifies, the DMS recommends and automatically deploys deceptions that are tailored to reflect what the organization has in its network. Decoys can include secure shell, remote desktop control servers, shared drives, browsers, and custom objects, artifacts, and more. The agentless technology does not install anything on real SWIFT systems, which is vital for SWIFT network elements. The core suite can be used to protect other financial applications, such as a trading system, by naming component assets and designing deceptions appropriate to the application.

## Context

The financial services industry was a rapid early adopter of deception technology providers over the last year or so because of increased attacks by cyber thieves. In April 2017, IBM's X-Force threat research team reported a 937 percent increase in the number of financial services records breached from 2015 to 2016. In fact, according to that X-Force report, the financial services industry was the top target, with the total number of records breached exceeding 200 million.[1] This sector was attacked 65 percent more than all other industries. The 2017 Verizon Data Breach Investigations Report also showed that the financial services sector was the top target among verticals, representing 24 percent of the breaches Verizon investigated.

Although organizations in the financial services industry range from small credit unions and regional insurance companies to global banks and investment houses, they all face the same business risks that come with big breaches: large financial losses, steep regulatory fines, and negative impacts on their organization's reputation. The movement of financial services applications to the web and the rise of mobile applications, including mobile banking, greatly expanded the attack surface for the sector.

Even well-defended networks such as the SWIFT messaging network can have chinks in their armor. As a result of attacks on multiple SWIFT participants, over $100 million was stolen in 2016. Any of the 11,000 organizations that use the SWIFT network, which carries 24 million messages a day, can serve as the weak link in the chain if they don't follow security best practices.

The X-Force study also found that the majority of attacks (58 percent) came from inside the organization, rather than from external threat actors. These internal attacks could be from malicious insiders or even from inadvertent acts in which an employee, while reading a phishing email, is tricked into opening an attachment containing malware or clicking on a link leading to a malware-infested site.

## EMA Perspective

The Bank of Bangladesh heist, which resulted in the loss of $81 million after cyber thieves hacked into the bank's SWIFT network, demonstrates that the menace of advanced persistent threats to banks is real and can be very costly.[2] Such attacks continue to target the range of financial services companies—even giants such as credit reporting agency Equifax, which recently revealed that cyber thieves stole personal information on as many as 143 million North American consumers. The Equifax breach may become the poster child for depicting the business risks associated with a serious breach, including direct revenue losses, regulatory fines, brand and reputation impacts, and legal implications (it took less than a day for a class-action lawsuit to be brought against Equifax). Furthermore, it may face increased regulatory burdens as well.

The timing of Illusive's emphasis on the financial services industry is smart, and fortuitous for organizations that have decided to leverage deception for early attack warning. Illusive brings unique advantages to the fight against cybercriminals. Its endpoint-focused approach to deception provides early visibility into the activities of attackers trying to gain access to sensitive resources and integrates incident analysis tools. This visibility identifies the attack path chosen and can lead to additional defensive strategies. Unlike traditional honeypots and honeynets, Illusive spreads decoy artifacts across all endpoints that can elastically expand and contract to increase the likelihood of early detection. This adaptive deception environment, enabled by the Deception Management System, is key in slowing or diverting the attack process, allowing response teams the time they need to keep the attackers from accessing their intended goal. This includes human attackers, automated attack scripts, and ransomware.

[1] 2017 IBM X Force Threat Intelligence Index: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03140USEN&
[2] Bank of Bangladesh heist

Other key benefits of the technology include:

- Full visibility into the actual risk to critical assets within the customer's network, which can be quantified and rolled up into APT attack risk metrics
- The ability to learn, using machine learning, how the customer's network behaves and then tailor deceptions to that network
- A forensics model that can collect information from the original source of an incident on activities that occurred before, during, and after the incident—without requiring an agent

For financial organizations of all types, time is money. By delaying the attackers, security teams give themselves the upper hand in controlling the attack clock, which is a luxury previously unseen.