Three Use Cases for Deception Technology in Financial Services

Black Hats vs. Top Hats

A white paper series on the use of deception technology to address industry-specific cyber risks

Financial Services

It's no surprise that the financial service industry plays such an important role in shaping best practices in cyber security. Banks, securities, and insurance companies—and increasingly, clearinghouses and other entities that enable the inter-dependent ecosystem—are in the crosshairs of attackers, both those who "follow the money" and those interested in causing systemic disruption. Despite the money, time and attention that financial institutions focus on cybersecurity, one challenge has been especially intractable: the challenge to detect APTs before real damage is done. Distributed deception technology is purpose-built to stop advanced attacks and, as discussed in this paper, also supports a wider range of incident handling activities that help align security operations to top business risks.

No amount of detection lag-time is acceptable

It is inherently difficult to identify adversaries moving around the network with valid credentials and sophisticated tools to cover their tracks—but amid the vastly complex environments of large financials, the rate of change, continuous business innovation, and other factors multiply the problem. Security operations teams, equipped with a sea of security tools, drown in data and alerts. While a lot gets detected, the highest-impact attacks can remain well-camouflaged.

Although the mean time to detect data breaches has declined somewhat[i], when acts of fraud, business disruption or IP theft can cause millions of dollars of damage in minutes or hours, no amount of lag-time is acceptable. Attacks need to be detected before, not after, high-value assets have been compromised, and incident responders must have information at their fingertips to determine what action to take.

Exposing an attacker's lateral movements

Distributed deception technology, designed from the viewpoint of the attacker to detect lateral movements toward high-risk data, applications, and systems, finally gives organizations an effective alternative — a way to regain control over the attack process.

A bad day doesn't have to be a crisis

With Illusive's particular approach to distributed deception, each endpoint becomes a trap. Once an attacker—whether insider or outsider—has landed on a system, his search for user credentials and routes to "Crown Jewels" leads him to reach for deceptions—false, but real-looking, information. Though they're unaware, they've triggered an alert. A forensic snapshot has been captured from their station. The incident is logged.

It is not a great day for incident responders, but it's not a crisis. Behind the scenes, a responder is equipped with the tools to know how far that attacker is from Crown Jewels and from being able to access domain admin credentials. An automated Deception Management System intelligently adjusts the deceptions. Information has been automatically shared with SIEM and other security tools. Because the attacker has been caught early in the process, responders have bought themselves time to analyze. They can take immediate action, or they can continue to watch his movements and gather information. The defender is in control.

On a good day

When not responding to critical events, security professionals can leverage Illusive's monitoring and risk visibility tools to proactively tighten up APT defenses and reduce the attack surface. Awareness of critical systems combined with continuous awareness of the endpoint landscape generates visibility on certain kinds of risk indicators that other technologies cannot detect. Such actions can include:

- Identifying potentially anomalous connections, compromised credentials, and users who may have unauthorized, elevated levels of access;
- Identifying areas where network segregation is not functioning as intended;
- Planning with business and IT groups to understand where new high-value assets may soon be introduced to ensure they are brought under Illusive monitoring in a timely manner;
- Scanning the network for new endpoints, servers, and connection pathways to ensure that deceptions are optimally deployed;
- Providing analysis and forensic support for incidents generated by other security tools;
- Providing APT risk metrics for upstream reporting to risk officers and business stakeholders.

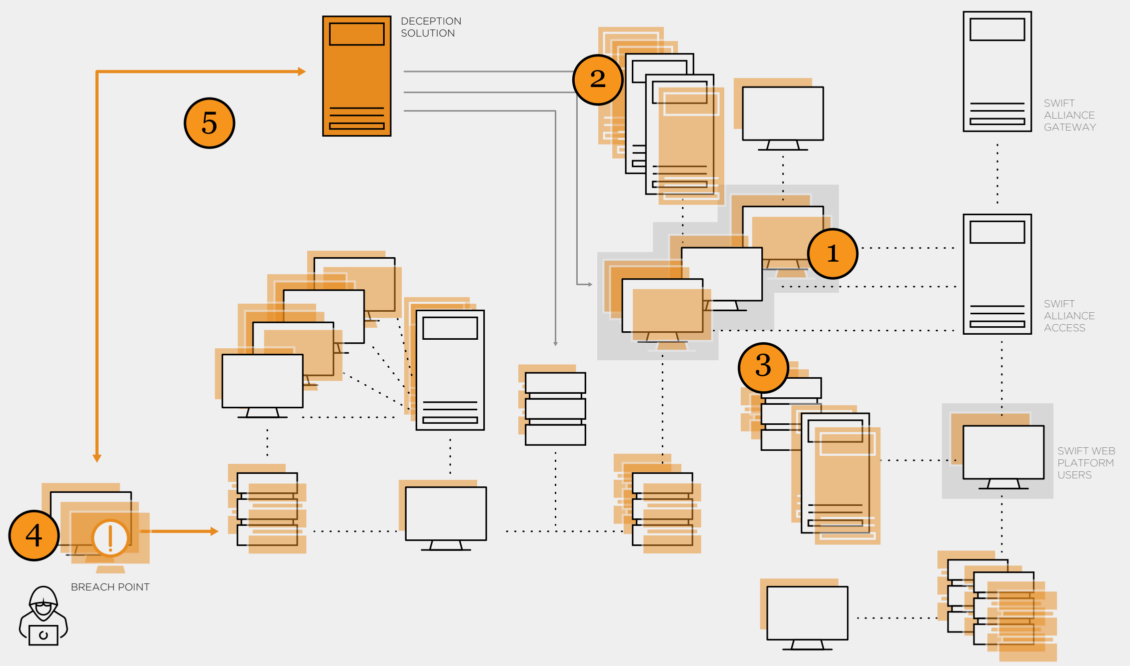
Agentless and equipped with intelligent automation, the Illusive solution is easy to deploy and requires little maintenance, even in highly scaled environments, and accommodates risk-oriented visibility on a wide range of business-critical systems, applications and processes. Below are some common deception use cases associated with risk management objectives in financial services companies.

Use Case #1: Guarding the integrity of wire transfers

On a typical day, the SWIFT financial messaging service delivers more than 25 million communications, helping to orchestrate some of the largest financial transactions in the world. Most wire transfer fraud is conducted APT-style: attackers move from one system to another, searching for the messaging systems. Once at their destination, they use valid credentials and carefully mimic the normal functioning of wire transfer components and processes to avoid detection. In the 2016 fraud attack on Bangladesh Bank, a $951 million would-be heist was truncated—only because a spelling error in one of the transaction messages raised the suspicion of a vigilant employee.

Preventing fraud in this case, whether perpetrated by an insider or an outsider, requires the ability to detect the thief's lateral movements before the wire transfer systems are reached. Illusive plants deceptions everywhere—everywhere except on wire transfer systems themselves, which are typically regarded as too sensitive to alter. Machines that can connect to the SWIFT systems are fitted with purpose-built deceptions that mimic fake SWIFT environments so that the attacker is forced to guess which one is real. No matter where an attacker first establishes a foothold in the network, a dense blanket of deceptions immediately creates very high odds that the attacker will unwittingly activate a deception and reveal himself[ii]. The solution is 100% non-intrusive to the real SWIFT environment.

How deception works to protect wire transfer fraud



1

Illusive automatically discovers the entire network, including hosts and servers that connect to the wire transfer systems, to understand how attackers can move from one place to another.

2

Deceptive information and objects (represented by orange shadows) designed to look like they'll help the attacker move toward wire transfer systems, are planted across the IT environment—everywhere except on the sensitive wire transfer systems themselves.

3

Special deceptions made to look like additional SWIFT systems (represented by grey shadows) are planted on the hosts that connect to SWIFT systems.

4

When an attacker breaks in to the network and begins to move laterally, the attacker will soon activate a deception, and an alert is triggered.

5

The deception solution instantly captures forensic data from the compromised machine, lets responders know the attacker's location, and provides various tools to support resolution of the incident.

Use Case #2: Defending legacy, custom or "untouchable" applications and systems

Reliance on cloud-based infrastructure, mobile customer engagement and payment methods, self-service investment tools, and other forms of fintech are all increasing the attack surface at a rate higher than security controls can keep up with. The need to put cyber strategies in place to protect a financial service company's most innovative applications and services gets well-deserved attention these days.

But behind the newer investments there are typically legacy applications and systems that either exist in parallel, or that directly provide core, business-critical transaction processing and data storage enablement to newer applications and services. IBM mainframe systems, for example, currently support 87% of all credit card transactions and enable 29 billion ATM transactions daily[iii]. Many operations rely on legacy

ERP implementations and custom applications of all sorts that, regardless of their age, would never pass basic security criteria today, but which cannot be easily replaced or upgraded because of risk of downtime and disruption.

While security controls may be very difficult or impossible to apply, these assets can also be difficult to monitor if they weren't natively designed to provide log data or do not easily integrate with log management tools. A deception approach is especially important when appropriate security design standards, traditional security controls, and monitoring functions are not feasible. But deception is more than a stop-gap measure. The entire environment — new and old alike— benefits from earlier detection of targeted attacks to protect the individual assets, and the business processes they support.

Deception for custom or legacy applications works the same way as for wire transfer systems, but extra care may need to be taken to ensure that Crown Jewel assets are thoroughly identified. Illusive provides an automated, "smart" deception design process for all commonly used operating systems, and a specialized, non-intrusive solution enhancement to cover mainframes. Deceptions for some types of business-critical, custom applications and assets can be manually tailored as needed, but Illusive's core, automated processes significantly reduce deployment time and ongoing management overhead.

Leveraging advanced automation to easily establish and scale layers of deceptions

Identify

Discover the endpoint environment and name "crown jewel" assets

Most discovery can be done through Illusive's automated process. A manual review should be done to ensure that all business-critical systems are identified, including assets throughout critical process chains. Once identified, Illusive maintains perpetual, adaptive visibility across all endpoints and Crown Jewels.

Design

Create deceptions appealing to the attacker

Deceptions mimic connection types, interfaces, application components, users, and other items that the attacker perceives as enabling movement toward key assets, and must blend with actual usage patterns in the environment to avoid being recognized by the attacker as fake. Using automated discovery, Illusive proposes tailored deceptions for all hosts and servers in the environment. Deceptions can be customized as needed to accommodate custom applications and legacy platforms.

Deploy

Disseminate deceptions

Once the design process is complete, Illusive's one-click deployment process automatically pushes them out across the entire enterprise infrastructure — without installing agents.

Manage

Ensure ongoing efficacy

The Illusive Deception Management System provides perpetual management of deceptions, and automatically refreshes and updates them to ensure that attackers cannot "learn" the environment, and adapts to changes in the IT environment and threat landscape.

A scalable, flexible architecture and advanced automation supports unique business requirements—even in large, global environments. The quality of the deceptions themselves—the essential objects installed across the endpoint environment to engage the attacker in advancing his attack process—is a critical factor in a strong deception solution. Illusive provides a highly automated, intelligent discovery, design and deception management process. Its flexible architecture enables tailoring needed to support older or custom-built applications, or other unique business requirements.

Use Case #3: Protecting through M&A and other disruptive business changes

In recent years, there has been growing concern that the discovery of a breach during or prior to due diligence could derail an M&A transaction. According to one survey report, "Seventy-eight percent of global respondents believe cyber security is not analyzed in great depth or specifically quantified as part of the M&A due diligence process, despite 83% saying they believe a deal could be abandoned if previous breaches were identified."[iv] Certainly, Illusive's nimble deception technology can be used leading up to a major business event to identify APT attack risk or reduce the risk of an advanced attack.

But the potential impact of cyber attacks on company valuation are only one part of M&A-related cyber challenges. Periods of IT change, especially the extended period of reconfiguring and consolidation in the wake of a merger or acquisition, can leave dangerous gaps that cyber attackers can readily exploit. It may also be a time when disgruntled or disenfranchised employees are most likely to commit acts of fraud or data theft, and when security personnel may be pulled into special projects that distract from routine patching and security maintenance. Certainly the post-transaction period is not a time when a business can afford a publicized cyber event, nor afford to divert IT security resources to a major crisis response effort.

A deception solution that can be deployed quickly and adjust automatically to the changing environment can play a significant role in protecting sensitive data and business-critical services during times of change and upheaval. This is an especially "sweet" spot for deception because it is, by nature, purpose-built to defend against high-impact attacks, knowing that even the best security controls will fail.

Not all deception technologies are up to this task, however. The solution must be capable of continuous or on-demand discovery of the diverse system environment to identify new hosts and changes to network and system usage patterns with little lag time. Deception design and ongoing management must be automated, as was discussed in the previous use case —and able to handle the growing scale of the business environment. The management interface must be able to accommodate broad visibility across the infrastructure, and also support granular incident response and anomaly investigation activity.

Illusive meets these criteria, and installs in days or weeks, depending on the scope of the network. Manual effort required is extremely limited, and deployment requires no agents or software changes on servers or endpoints. When an alert fires, forensic data is instantly captured from the compromised host and immediately tied to the incident record so that responders can assess and act quickly.

In Closing

The three use cases described above are only some of the ways financial services companies can apply a deception approach. To help their organizations thrive, business leaders must reshape their security programs to mitigate the cyber risks associated with digital transformation and technology-driven business models. A deception solution is more than just another tool in a controls-focused, layered defense model; it helps lay the foundation for an active defense program that acknowledges the reality that in today's dynamic, hyper-connected world, attackers are always present.

Deception technology has come a long way since the early days of labor-intensive, manually-built honeypots. Illusive is a state-of-the-art deception solution built on intelligent automation to deliver nimble, low-maintenance solutions for reducing the risk of cyber disruption to critical finance industry operations by stopping advanced attacks before an attacker, once inside, can effectively strike.

[i] *Ponemon Institute's 2017 Cost of a Data Breach* (June 2017) indicates that the overall Mean Time to Identify (MTTI) a data breach declined by slightly between 2016 and 2017 (from 201 to 191 days)

[ii] Mathematically, there is a 99% likelihood that the attacker will be caught within three lateral movements following his initial act of compromise

[iii] *IBM Mainframe Ushers in New Era of Data Protection,* July 17, 2017 http://www.prnewswire.co.uk/news-releases/ibm-mainframe-ushers-in-new-era-of-data-protection-634874243.html

[iv] *Cyber Security in M&A,* Freshfields Bruckhaus Deringer LLP, July 2014

For additional resources or to subscribe to our blog, please visit us at www.illusivenetworks.com

For more information about the Illusive's Deceptions Everywhere® approach and the Illusive Core Solution, visit https://www.illusivenetworks.com/deceptions-everywhere

For more information about solution enhancements for financial services companies, please see: Illusive Mainframe Guard

And Wire Transfer Guard products, visit https://www.illusivenetworks.com/wire-transfer-guard

Visit our https://blog.illusivenetworks.com/ blog
and our https://www.illusivenetworks.com/collateral resources page for articles on red teaming
and other best practices for deception in the financial services industry

To discuss your unique business requirements,
please call us or email info@illusivenetworks.com

United States and Canada	Outside the US
+1 844.455.8748	+972 73.272.4006

Follow Us:

About Illusive Networks

Illusive Networks is a pioneer of deception technology, empowering security teams to take informed action against advanced, targeted cyberattacks by detecting and disrupting lateral movement toward critical business assets early in the attack life cycle. Agentless and driven by intelligent automation, Illusive technology enables organizations to significantly increase proactive defense ability while adding almost no operational overhead. Illusive's Deceptions Everywhere® approach was conceived by cybersecurity experts with over 50 years of combined experience in cyber warfare and cyber intelligence. With the ability to proactively intervene in the attack process, technology-dependent organizations can preempt significant operational disruption and business losses, and function with greater confidence in today's complex, hyper-connected world.

Copyright © 2017 Illusive Networks. All rights reserved.