illusive

SOLUTION BRIEF:

Wire Transfer Guard™

illusive

The Emerging Threat Of SWIFT Attacks

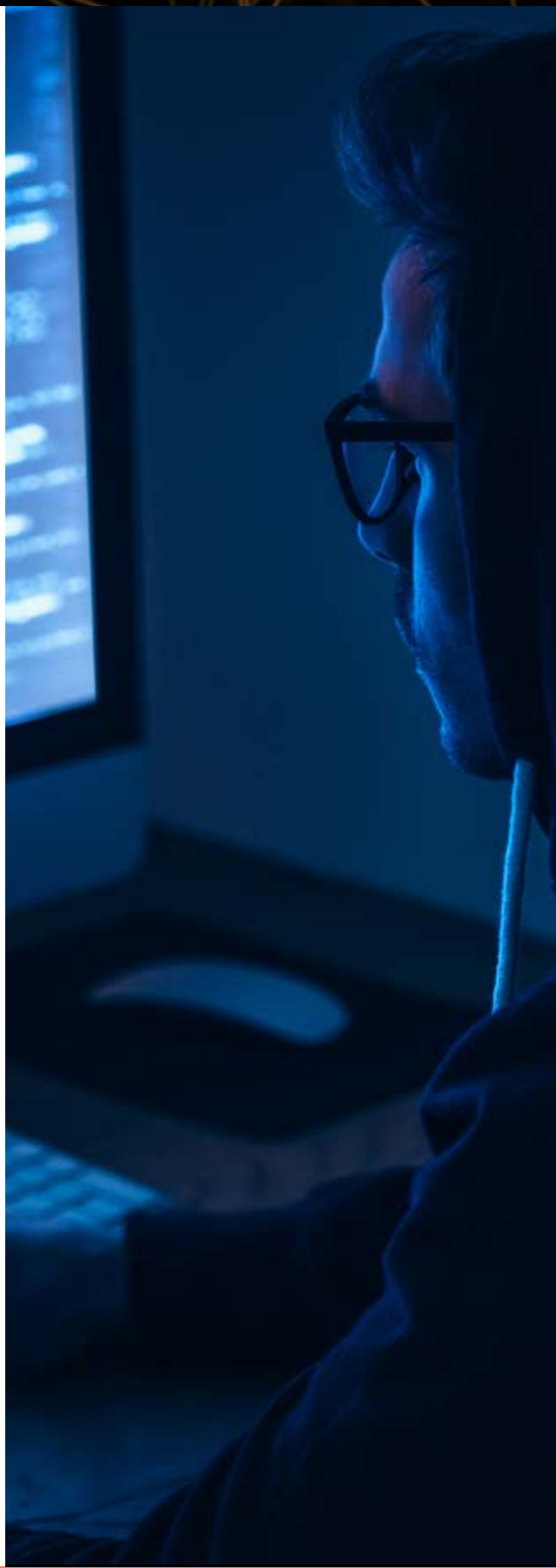
Every day, SWIFT handles over 25 million money-transfer messages involving billions of dollars.

SWIFT attacks are becoming a major concern to the financial industry as more and more cyber attacks are targeting SWIFT systems.

The SWIFT financial messaging service, provided by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), is used by over 11,000 institutions across 212 countries. With such a broad footprint, sophisticated cyber criminals are increasingly attacking SWIFT systems to steal large amounts of money without being detected.

The first known major SWIFT attack was executed in February 2016 against Bangladesh Bank. Attackers performed APT lateral movements for one year before reaching the bank's SWIFT system. They used one of the bank's SWIFT servers and an Oracle database to generate unauthorized SWIFT messages, then covered their tracks by preventing records from being printed. Of the attempted $951 million in fraudulent transfers, the heist saw **$81 million stolen** before an employee spotted a spelling error by happenstance and raised the alarm.

In 2016 alone, more than a dozen banks worldwide suffered SWIFT attacks. Between January and July 2016, SWIFT attacks are estimated to have stolen **over $100 million**.



"THE THREAT IS PERSISTENT, ADAPTIVE, AND SOPHISTICATED – AND IT IS HERE TO STAY."

SWIFT organization on SWIFT attacks, Aug 30, 2016

illusive

Wire Transfer Guard™: The First Deception-Based Solution Built To Protect SWIFT Networks

The illusive Wire Transfer Guard™ protects your business, finances, and brand by stopping SWIFT attacks before they start. The solution identifies and suppresses SWIFT attacks long before SWIFT assets are breached, triggering alerts that keep you one step ahead of attackers: safe and in control.

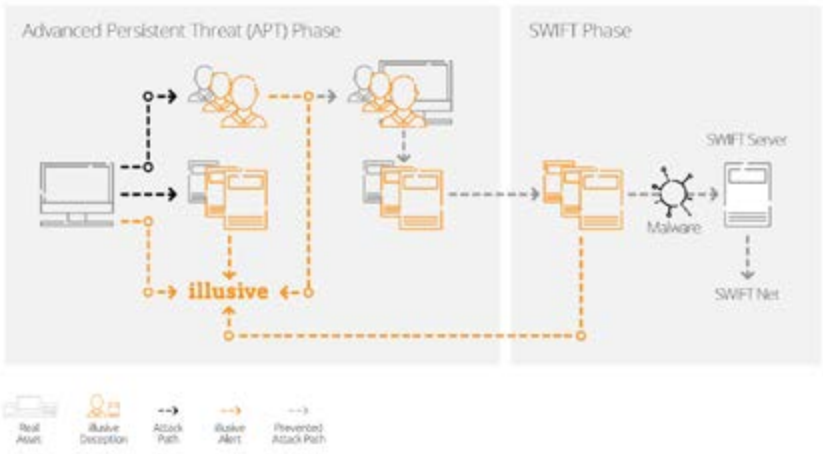
To locate a network's SWIFT system, attackers use APT techniques, diligently discovering the network by moving laterally from host to host. Once SWIFT assets are identified, protocols and processes are revealed, monitored, and mimicked, allowing attackers to steal large amounts of money below the organization's radar.

How Wire Transfer Guard™ Can Secure Your SWIFT Network

illusive provides a unique security solution for the financial industry, with complete protection across all attack stages, ensuring detection during APT movements and attack suppression during SWIFT-system access attempts.

Wire Transfer Guard™ coats a financial organization's network with dedicated deceptions that appear identical to real wire transfer assets. To stop attacks during preliminary network exploration, deceptions mimic real systems and entities, appearing as credentials, servers, interactive gateways, and many other wire transfer components. When attackers first stumble upon these unavoidable deceptions, the attack is diverted and revealed while real-time forensics are collected from compromised hosts.

SWIFT Attack - Prevention Through Deception



BENEFITS

- Visibility into your SWIFT ecosystem
- SWIFT-attack risk analysis
- Early, reliable attack detection
- No added total cost of ownership (TCO)
- Risk-free, with no impact on business operation
- Supports all SWIFT software versions
- Agentless

"BY 2019, CONTINUED WEAKNESSES IN PREVENTION WILL DRIVE **AT LEAST 10% OF LARGE ENTERPRISES TO ADOPT DECEPTION-ENABLED TOOLS AND TACTICS** (UP FROM JUST 5% IN 2016), IMPROVING DETECTION AND RESPONSE, AND SHIFTING SOME OF THE ECONOMIC BURDEN TO ATTACKERS."

- Gartner Competitive Landscape: Distributed Deception, August 2016

illusive

The illusive Difference: Deceptions Everywhere®

illusive exposes attackers by turning their strengths into weaknesses. The revolutionary illusive networks Deceptions Everywhere® solution weaves a deceptive layer over your entire network, creating an environment where attackers cannot rely on the information they collect. If attackers cannot collect reliable data, they cannot make decisions. And if they cannot make decisions, the attack is paralyzed.

As deceptions are invisible to valid users and systems, no false-positive alerts are triggered; every notification of deception use is a high-fidelity indication of an attack.

illusive's actionable alerts provide the real-time forensic information needed to investigate and contain attacks. Information is collected from compromised hosts at the exact moment that attackers use false data, before they have time to clean their tracks.

Using the illusive Deception Management System™ (DMS), deceptions are automatically optimized, instantly diversified, and constantly monitored. The agentless technology ensures zero impact to business operations and working environments.

Revolutionary Visibility: Attacker View™

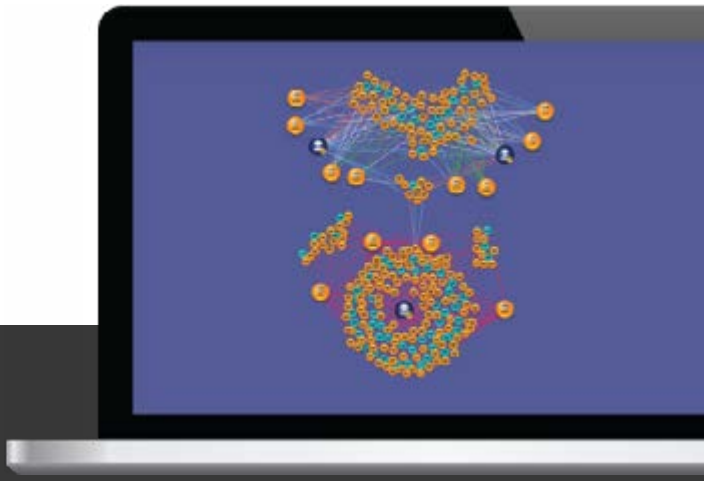
The illusive Attacker View™ is a powerful application that displays your network as attackers see it. The Attacker View is a groundbreaking tool, enabling you to evaluate your network's cyberattack risk status, map discoverable and reachable sensitive assets, minimize attack paths, and mitigate remaining risks via deception policies. Additionally, the Attacker View produces an Attack-Risk Report to help you manage your organization's safety.

"ILLUSIVE NETWORKS IS A PERFECT EXAMPLE OF THE KIND OF 'OUT OF THE BOX' THINKING NECESSARY TO CHALLENGE THE GROWING THREAT OF TARGETED ATTACKS."

-Eric Schmidt, Google Chairman and Founding Partner at Innovation Endeavors

A UNIQUE APPROACH

- illusive's Deception Management System™ (DMS) automatically manages, distributes, and monitors dynamic deceptions
- Attackers reveal themselves long before reaching sensitive data
- The Attacker View™ reveals hidden attack paths before attacks occur
- The earliest attack alerts in the industry
- Highest-fidelity alerts available
- The most detailed, real-time source-based forensics attainable



ABOUT ILLUSIVE NETWORKS

illusive networks is a global pioneer of deception technology – the most effective protection against advanced attacks. To lead the Distributed Deception Platform, top cyber-attack specialists from Israel's elite cybersecurity Intelligence Corps (unit 8200) were brought together with pioneering experts and entrepreneurs with over 50 years of combined experience in cyber warfare and cybersecurity.

With offices in Tel Aviv and New York, illusive networks changes the asymmetry of cyber warfare by focusing on the weakest link in a targeted attack – the human team behind it.

For more details, visit **www.illusivenetworks.com** or contact info@illusivenetworks.com.