WHITEPAPER

Attivo NETWORKS®

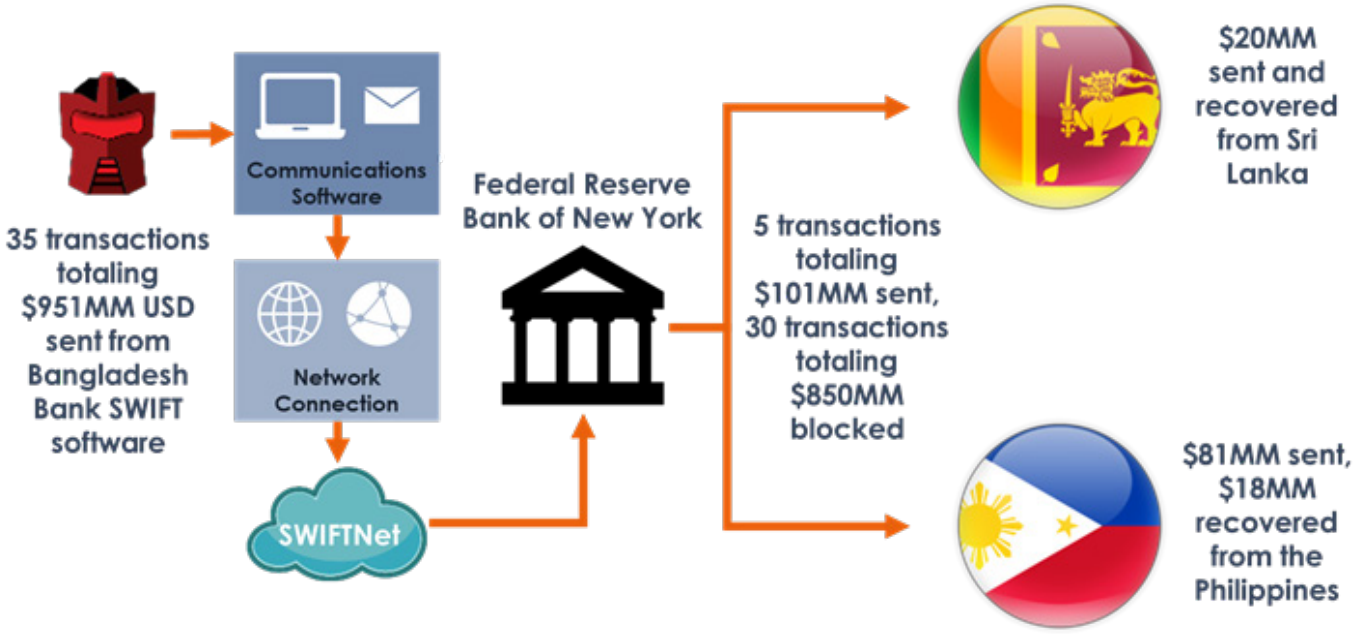
DECEPTION FOR A SWIFT DEFENSE

PROTECTING FINANCIAL MESSAGING SYSTEMS

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) system is a network that enables financial institutions to send and receive information about financial transactions in a secure, standardized, and reliable environment. The SWIFT network links more than 11,000 financial institutions in more than 200 countries and territories worldwide, and as such, requires a level of trust between member institutions to ensure the integrity of the network. The SWIFT financial network is a closed system with well-integrated internal security, and as such, banks view messages sent via the SWIFT network as inherently trustworthy. Unfortunately, the SWIFT network has increasingly become a target of attackers over the past few years and traditional security measures are no longer sufficient to deter and stop attackers.

SITUATION OVERVIEW: ATTACKS AGAINST THE SWIFT SYSTEM

The BDA SWIFT bank heist in 2015 and the Bangladesh Bank heist in 2016 are just two recent attacks that have targeted the SWIFT network. Over a 10-day period in January of 2015, a secure computer terminal at Banco del Austro (BDA) in Ecuador sent 12 messages instructing San Francisco-based Wells Fargo to transfer a total of $12 million to bank accounts across the globe. The attackers had obtained a BDA employee's SWIFT credentials and accessed previously cancelled or rejected SWIFT requests from the bank's SWIFT outbox. They then altered the amounts and destinations on the transfer requests and reissued them.[1] BDA discovered the theft over a week later, but by then the money was gone.



Over a local holiday weekend in February of 2016, attackers sent 35 SWIFT messages to the Federal Reserve Bank of New York with instructions to wire a total of $951 million from Bangladesh Bank, ultimately taking off with $81 million. The attackers successfully installed malware on the SWIFT terminal that allowed them to modify the database that logged the bank's activities over the SWIFT network. They deleted outgoing transfer requests and intercepted incoming confirmation messages for the transfers. The malware also let the attackers manipulate account balances to hide the theft and hide printer output of the requests.[2] Investigators suspect that as many as 12 other banks in Southeast Asia have been targeted by the same group of attackers, and other attacks have followed since. In an interview with Reuters in December 2016, Stephen Gilderdale, head of SWIFT's Customer Security Programme stated that banks using the SWIFT network, which include both central banks and commercial banks, have been hit with a "meaningful" number of attacks - about a fifth of them resulting in stolen funds, since the Bangladesh heist.[3]

These two incidents illustrate the ways attackers can commit fraud through the SWIFT network. In the first incident, attackers managed to steal credentials with access to send messages through the SWIFT terminal, impersonating a legitimate user, thereby bypassing the security controls entirely. Since a legitimate user sent the messages, the recipient bank had no reason to question the funds transfer requests. In the second incident, attackers crafted malware that targeted the reporting functions of the SWIFT terminal in addition to gaining credentials with access and authorization to send funds via SWIFT. This way, the attackers were able to circumvent the manual checks the bank had put in place to confirm SWIFT requests, hiding their activity until it was too late. Were it not for a misspelled word in some of the requests, the $81 million in funds could potentially have been $951 million. While there is lingering suspicion that insiders may have been involved with the theft, common to most of these incidents is the use of stolen credentials to send SWIFT messages.

CHALLENGES DEFENDING SWIFT

Defending the SWIFT banking network presents unique challenges. Financial institutions often find it challenging to update and patch wire transfer mission-critical systems quickly. Because banks require 24-hour uptimes to support global banking, taking down a SWIFT terminal can lead to delays in processing transactions from a partner bank. Additionally, it is difficult for financial institutions to understand where attackers will come from, the paths they will take to attack SWIFT systems, and how to effectively block such avenues of attack. Even if they could map such

PRIMARY CHALLENGES

- Credential theft detection
- Updating and patching systems
- Fluid attack paths
- Vulnerabilities at member banks

routes, there is no guarantee that the routes would remain static, as new systems and users join the network. These challenges result in standard prevention technologies being unsuccessful in adequately addressing the needs of a SWIFT security environment.

Another factor attackers can exploit to attack the SWIFT system is that many smaller banks in underdeveloped countries do not have the cyber resources as banks in more industrialized countries. While these smaller banks, such as Bangladesh and Ecuador, have borne the brunt of attacks so far, larger banks in Taiwan have also been hit.[4] Banks connected to the SWIFT system are exposed to risks because of the security vulnerabilities of other member banks. While SWIFT has begun making changes to combat attacks aimed at the network, member financial institutions can use deception technology as another layer of defense to protect themselves from becoming victims.

SUMMARY OF SWIFT SYSTEM RISKS

- Attackers managed to steal credentials with access to send messages through the SWIFT terminal, impersonating a legitimate user, thereby bypassing the security controls entirely. Since a legitimate user sent the messages, the recipient bank had no reason to question the funds transfer requests.

> The element of surprise is no longer the foundation of deception.

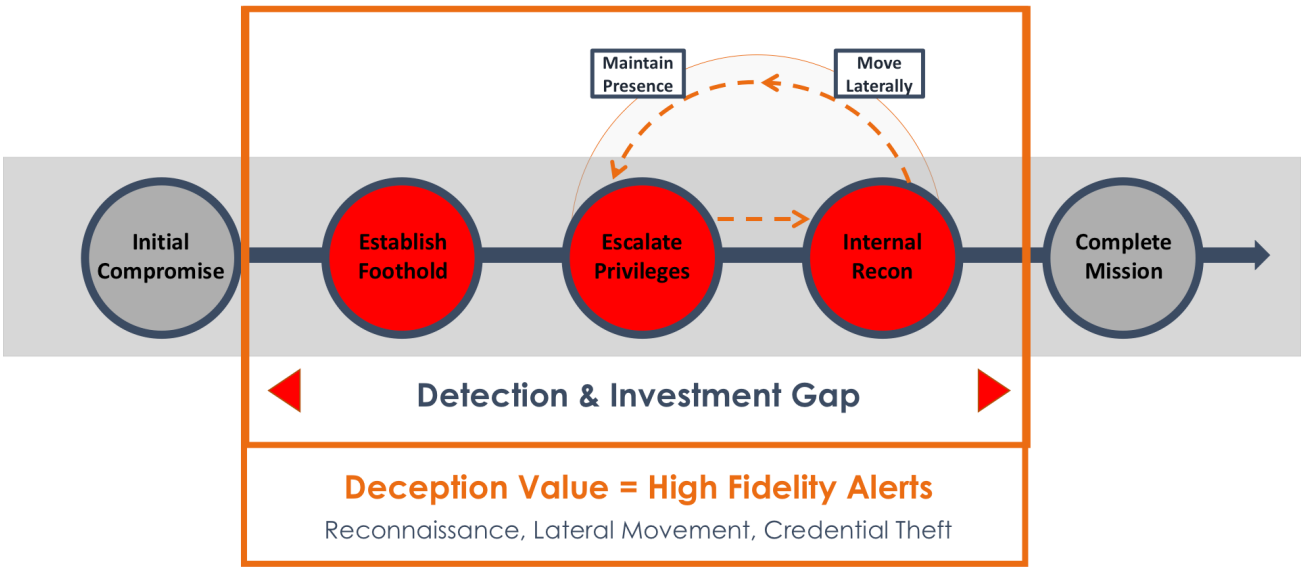
- It is difficult for financial institutions to understand where attackers will come from, the paths they will take to attack SWIFT systems, and how to effectively block such avenues of attack.
- Many smaller banks in underdeveloped countries do not have the cyber resources as banks in more industrialized countries.

DECEPTION TECHNOLOGY FOR SWIFT SYSTEM ACTIVE DEFENSE

Financial organizations are actively turning to deception technology as the preferred security control for early and accurate detection of threats that have bypassed other security controls. Some are first-time deception technology adopters, drawn to the accuracy and efficiency of the solution, while others are migrating off homegrown honeypot technology for additional accuracy and operational efficiency. Deception technology works by turning the network into a web of sensors with a maze of misdirection that tricks an attacker into engaging and revealing their presence. In a deception network, the attacker need make only one small engagement mistake to reveal their presence. By being present at the network and endpoint layers, deception technology blankets the network with lures and traps designed to attract and engage an attacker during reconnaissance, lateral movement, while harvesting credentials or when

seeking to compromise Active Directory. Deception technology only generates an engagement-based alert that is substantiated with threat and adversary intelligence, making such detections accurate and immediately actionable.

Advanced Distributed deception platforms can also go beyond detection and into providing an Active Defense that enables the ability to safely engage with the attacker and accelerate incident response. With built in sandbox technology, organizations will save time and energy with automated analysis of each attack, capturing of the attacker's valuable Tactics, Techniques, and Procedures (TTPs) and Indicators of Compromise (IOC) and by being able to communication with Command and Control to pick up new instruction sets and signatures. This actionable intelligence can then be applied reducing mean time to remediation and to better fortify the network.



DECEPTION FOR CLOSING THE DETECTION GAP THROUGHOUT ATTACK PHASES:

- **ESTABLISHING A FOOTHOLD AND PRIVILEGE ESCALATION** – After initially compromising a system, attackers will attempt to establish a foothold in the environment. They will seek to establish reliable communications with Command and Control (C&C) servers outside of the environment and will often utilize custom malware to install back doors and remote access tools to maintain initial access, as well as steal credentials stored on the system to reuse later in their attack. These types of activities are difficult to detect, as attackers can hide their C&C communications several ways.

- **CREDENTIAL THEFT AND PRIVILEGE ESCALATION** – Detecting valid credential theft and reuse is extremely difficult, especially if the attacker does nothing out of the ordinary for those credentials. Some common techniques used to harvest credentials are:

  a. Using tools to harvest a user's passwords, hash, or Kerberos ticket from memory, or from applications like Outlook, database clients, browsers, FTP clients, and others.

b. Performing Man-in-the-Middle (MitM) attacks to intercept credentials in transit.

c. Active Directory attacks as a method to gain information on credentials and organizational structure.

After harvesting legitimate credentials from an endpoint, the attacker can move from system to system, gathering and using more credentials until they gain administrative or privileged access and rights. Because the intruder uses real credentials, it is extremely difficult for most traditional security devices to detect the attacker.

Deception systems play an essential role in credential theft and privilege escalation detection by feeding misinformation to the attacker that seeks to steal credentials. Endpoint-based deception places attractive deceptive credentials that appear as ones of a legitimate user or a network shared drive on an endpoint or server with the goal of enticing the attacker to steal them. The moment an attacker attempts to use the deceptive credential, they are led to a deception server where the platform raises an alert, reveals the presence of the attacker, and analyzes attack activity. The platform can also open communications with C&C systems to gain additional insight into the attacker's tools, methods, and communications.

> Analysts can use the threat intelligence dashboard to drill down into specific threat detail and clickto-activate blocking and quarantine actions driven by integrated 3rd-party solutions.

Network decoys can detect MitM attacks that try to capture credentials in transit. Since MitM activity is passive by nature, it is very difficult for traditional security solutions to detect them, as they must be on the same subnet as the MitM attacker to detect the activity. Because network decoys can be deployed to any subnet, they can passively listen to unusual traffic that can indicate MitM activity and alert the security team to it.

- **INTERNAL RECONNAISSANCE** – Attackers will conduct internal network reconnaissance to identify high-value targets or assets with digital proximity to critical financial systems such as SWIFT terminals. Internal reconnaissance actions by the attacker can go undetected because they are conducted over a period of weeks or months, blending in with the "normal" traffic on the network. Some reconnaissance activity, such as directly querying Active Directory from any member system to reveal system and user accounts or trusted domains, will yield vast amounts of information without alerting anyone.

  Organizations can place deception decoys strategically to appear as production assets, and plant deception lures to attract attackers into engaging. They can also incorporate deception into Active Directory. Any attempt by

an attacker to conduct reconnaissance or scan a network deceptive asset will trigger an alert. Querying Active Directory will result in harvesting deception user and system results along with the production results while helping validate the stolen credentials as they will have matching records in the Active Directory database.

- **LATERAL MOVEMENT** – Attackers use lateral movement in different ways. They use lateral movement to enable credential theft and escalate privileges, as different systems may contain higher-privileged credentials. They conduct critical system reconnaissance by moving to different systems on the network and examining them to identify their role, making use of the stolen credentials they have gathered in previous attack phases. Identifying these systems is essential for subsequent attack phases, as they can contain databases, sensitive files, unreleased code, or other critical information. Lateral movement can even enable malware spread, such as a worm or ransomware.

  Network-based deception plays a key role in detecting lateral movement, especially when combined with endpoint-based deceptive credentials. As attackers move from system to system or follow credentials to other systems, they can interact with the network decoys, giving organizations advanced warning early in the attack cycle.

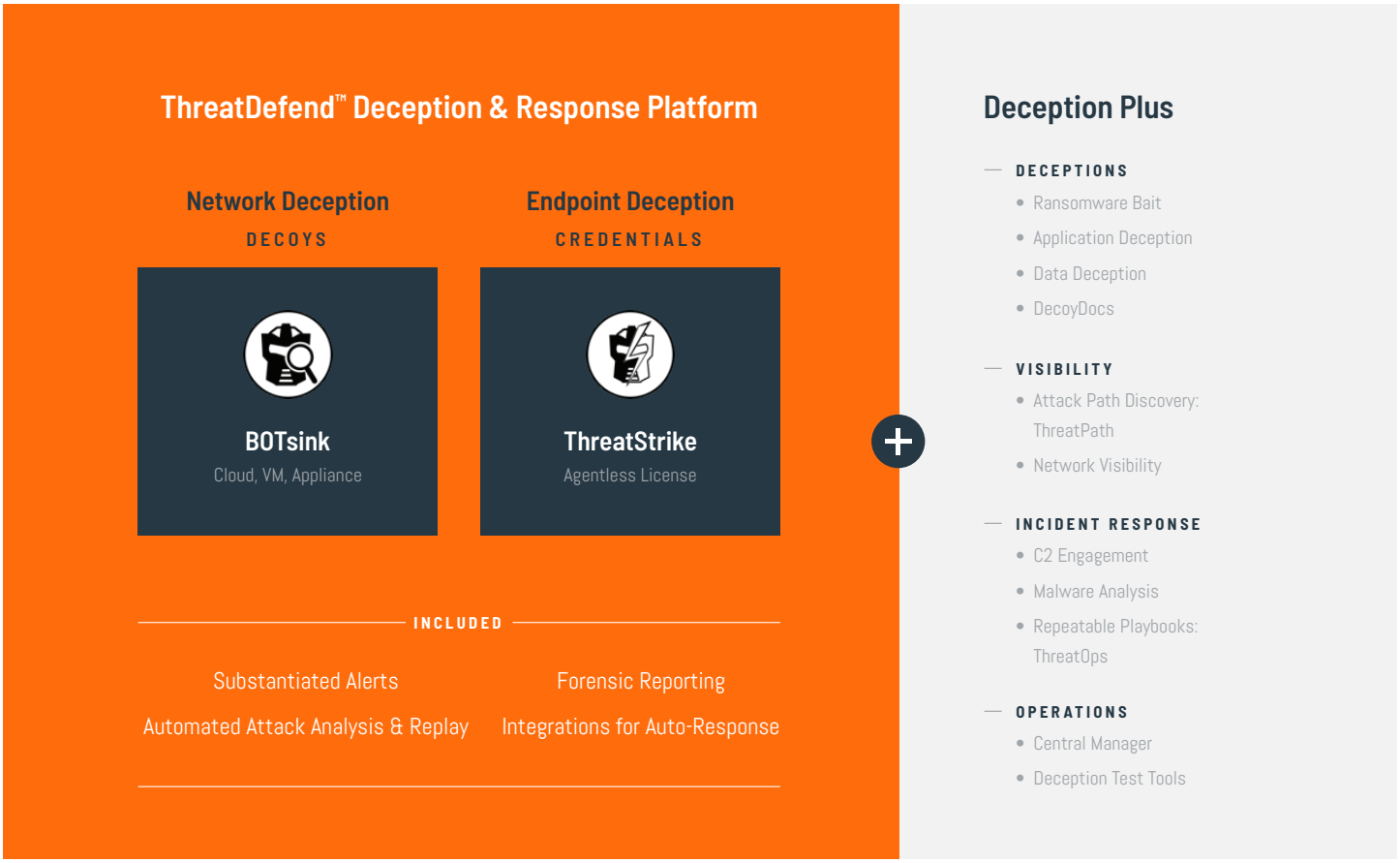
  > Attivo blankets the environment with deceptive credentials to engage attackers as they progress.

  In the event of a ransomware attack, high-interaction deception will feed fake data to the ransomware to keep it continually encrypting. This provides the security teams a time advantage to stop the attack by isolating it from the network before it can cause mass harm.

  Without deception, detecting lateral movements inside the network (east-west traffic) is extremely challenging. An active deception platform can accurately detect lateral movement, even with sleeper and time-triggered agents. From lateral movements originating on an endpoint (because of a malicious email) to those activated at the database tier (from an exploited web application) to MitM attacks at all levels of the network, deception can detect these activities.

- **MISSION COMPLETION** – It is critical for an organization to prevent an attacker from exporting sensitive financial or company data from a network or sending fraudulent funds transfers. Deception platforms provide valuable insight that cannot be gathered by tools that only block or detect an attack. With the ability to gather information about the attack's payload, its activities, and communications from C&C, deception platforms can not only detect, but also collect, analyze, and report on attacks to identify exfiltration. Within the platform, the attack plays out

in a controlled "synthetic" environment that collects attack information. By collecting data from C&C servers the attacker communicates with, the organization can preemptively block those addresses with existing perimeter security tools, preventing data exfiltration. The solution can be instrumental during polymorphic attacks since it will continue to update signatures generated over time based upon time-triggered C&C communications. The solution can also capture the destination accounts used in fraudulent funds transfers when the attacker inputs them into the decoy SWIFT systems.



ATTIVO THREATDEFEND DECEPTION AND RESPONSE PLATFORM

Attivo Networks is consistently recognized for its innovation and leadership in deception-based information security defense. The company's heritage and leadership reside in not only detecting, but also in responding to both human and automated attackers. The company's ThreatDefend Deception and Response Platform is designed for an evolving threat landscape and attack surface of user networks, data centers, cloud, and specialized environments like IoT, SCADA, POS, telecom, and medical devices.

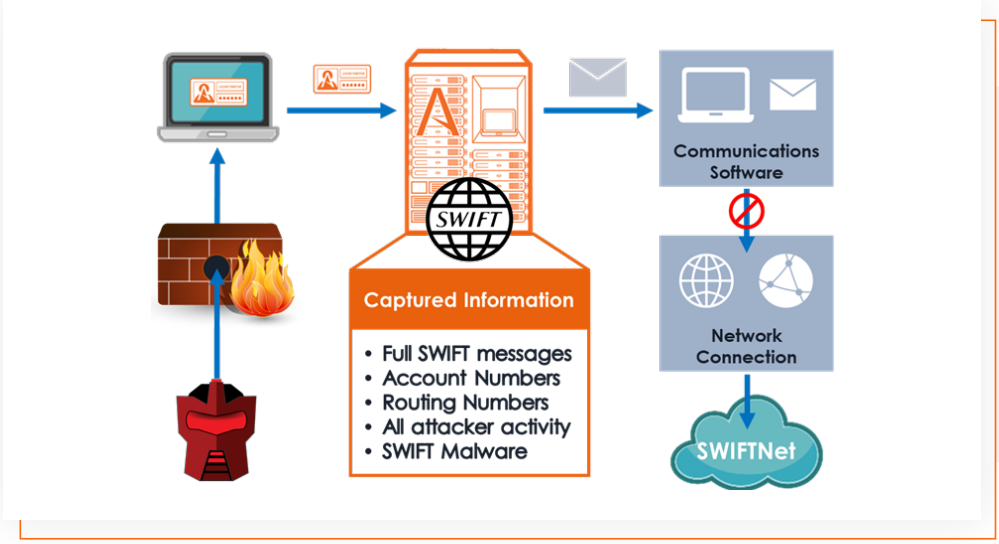
Offering the most flexible and comprehensive solution with support for network, credential-based, and Active Directory threat detection, Attivo Networks has become the detection technology provider of choice for many financial institutions based on the ThreatDefend Deception and Response Platform's ability address the following:

SWIFT DECEPTION

- Create SWIFT terminal decoy servers by importing a SWIFT system image, installing the SWIFT software onto a decoy system, loading the SWIFT web page front-end onto the deception engagement server's web service, or using the included default SWIFT front-end web page template.
- Customize the decoy to appear as a production SWIFT system.
- Create ThreatStrike SWIFT credentials pointing to engagement servers with SWIFT-based content.
- Capture message contents entered on the decoy SWIFT terminal to identify accounts used for fraud.
- Alert for any attempts to load SWIFT-related malware.

FLEXIBLE DEPLOYMENT AND OPERATIONS

- Bolster endpoint defense with agentless deceptions designed to plant credential and ransomware lures.
- A wide variety of deployment options including software deployment models (SCCM, WMI, group policies, login scripts) and endpoint management tools (ePolicy Orchestrator, Tanium, Casper, CounterAct, and others).
- Flexible out of band deployment in appliance, VM, or cloud configurations, modular design facilitates seamless expansion of new functions.
- Machine learning for automated deployment, deception campaign proposals, and automated deception refresh.
- Scale and provide operationally efficient deployments for large global networks.



DECEPTION FOR SWIFT FINANCIAL MESSAGING SYSTEMS

AUTHENTIC AND ATTRACTIVE DECEPTION

- Set highly authentic and interactive traps and lures to detect threats from human (APT, insiders, 3rd-party) or automated (malware, scripts, bots) attackers.
- Detect all threat vectors, including phishing, zero-day exploits, unpatched systems, stolen credentials, end-point/ BYOD, and website downloads.
- Efficiently detect lateral movement, network, and Active Directory reconnaissance, credential harvesting, ransomware, and Man- in-the-Middle attack.
- Detect zero-day and advanced threats with no dependency on signatures, known attack patterns, or database queries.
- Application and data deceptions to attract in-network threats away from production assets.
- DecoyDocs to attract attackers, for data loss tracking, and counterintelligence.

ALERTS, ANALYSIS, AND FORENSICS

- Deliver only high-fidelity, real-time alerts triggered by attacker detection and engagement.
- Gather and correlate the full TTPs and IOCs of an attack for threat and adversary intelligence.
- Attack threat analysis engine for automating attack correlation and generating forensic reports.
- Full forensic capture of all attack activity on the decoys at the disk, memory, and network layers.
- Provide downloads for all network packet captures and files dropped in the decoys.
- Built in Malware Analysis Sandbox for automated malicious binary examinations.

INCIDENT RESPONSE

- Provide a threat intelligence dashboard for a centralized view of all alerts and actionable drill downs for simplified incident response.
- Create repeatable incident response playbooks using the ThreatOps module.
- Accelerate incident response (block, isolate, threat hunt) through 3rd-party integrations with firewall, NAC, end-point, and SIEM vendors.

NETWORK VISIBILITY AND ATTACK PATHS

- Provide visibility into insider, contractor, supplier, and partner 3rd-party threats as they conduct reconnaissance and move laterally through networks.
- Network visibility for device adds, changes, and location of deception assets.

- Show attack time-lapsed replay for understanding attacks and strengthening defenses.
- Identify and graphically show misconfigured, misused, or orphaned credentials to shut down credential-based attack path vulnerabilities.

COUNTERINTELLIGENCE

- DecoyDocs provides the ability to plant deception files that allow the organization to track documents that were exfiltrated via a callback function. The callback provides the externally facing IP address and geolocation of every system that opens the file thereby providing data that can help with attribution, identification, and proactive security measures.

WHAT MAKES ATTIVO DECEPTION UNIQUE

AUTHENTICITY

The element of surprise is no longer the foundation of deception. For today's anticipating attacker, authenticity plays a key role in attracting an attacker's attention, but also in avoiding their detection. The Attivo Deception and Response Platform, based on its Camouflage Deception techniques and Adaptive Deception Campaigns, lures the attacker by running real operating systems and production golden images. These capabilities are used to fool attackers by customizing decoy engagement servers to be indistinguishable from production assets, luring attackers away from production systems.

Additionally, the solution uses machine learning to create Adaptive Deception Campaigns. These self-learned deception campaigns enable automatic credential and decoy refresh based on a schedule or suspicion of an attack that may be underway. Decoys can be automatically set to not only rebuild, but re-spin after attacker engagement to avoid fingerprinting.

AUTOMATED ATTACK ANALYSIS AND RESPONSE

Attivo Networks recognizes that detection is only the first step in incident handling and provides the tools required to promptly respond and address the situation. All alerts are evidence-based with the substantiated, actionable detail required to identify the infected device and understand the attacker's actions, including gathering external IP addresses, tools, and methods when the attacker establishes Command and Control communications. With these actionable attack details, security analysts can now quickly and confidently quarantine a device and remediate an attack.

The ThreatDefend Platform includes an attack threat analysis (ATA) engine that provides automated attack correlation and forensic-based threat reporting for all activity that occurs in the deception environment. The ATA collects full threat TTPs, including payload drops, registry changes, identified malware propagation methods, and SHA-1 signatures. The ATA engine tracks and records the attacker's actions for forensic evidence reporting.

The Malware Analysis Sandbox (MAS) is a decoy converted into a dedicated binary analysis VM that analyzes any suspicious executables from phishing emails, potential malware, and other threats to capture lateral movement methods, observe malware behavior, and identify attacker IP addresses such as Command and Control IPs on the Internet. The MAS provides automated, in-depth malware binary and phishing emails analysis, removing hours of time that would traditionally be dedicated to testing binary files.

The MAS can be particularly useful for security teams seeking to protect high-profile executives from targeted phishing attacks through its automated mail analysis function. Security teams can configure the MAS to accept email submissions and provide users with a simple mechanism for submitting samples for review. When incorporated as part of an annual phishing awareness training campaign, recognizing and submitting suspicious emails becomes a matter of simply clicking a button on the email client.

> Deception systems play an essential role in credential theft and privilege escalation detection by feeding misinformation to the attacker that seeks to steal credentials.

Analysts can use the threat intelligence dashboard to drill down into specific threat detail and click-to-activate blocking and quarantine actions driven by integrated 3rd-party solutions. The platform can easily create and share attack information and details through IOC, PCAP, STIX, CSV, and other reporting formats. The platform also provides 3rd-party integration with SIEM solutions like Splunk, ArcSight, and QRadar along with integrations for popular firewalls, NAC, and endpoint software to automatically block, quarantine, and remediate infected devices. Additional integration with companies like CarbonBlack, ForeScout, and McAfee support threat hunting and information sharing.

COUNTERINTELLIGENCE

In addition to understanding what and how the attacker conducts operations, it becomes increasingly valuable to understand what information they are looking for, how they are collecting it, and where it goes. Attivo data deceptions include a tracking mechanism to understand where a file ends up and empowers the organization to know where to plant fake documents. These documents can be used to create doubt as to the integrity of what was stolen, which slows an attacker and increases their costs as they now need to validate the integrity of the stolen assets.

The value of this deception mechanism lies not only in tracking what was taken, but in identifying when an insider gains unauthorized access to sensitive data. The tracking mechanism works both inside and outside of the network. Insiders seeking to take advantage of illicitly acquired sensitive data can be duped into accessing a tracked document, unknowingly alerting the security team who can act to prevent further unauthorized access.

SCALABILITY

Deployment of the ThreatDefend platform is, by design, highly scalable. The BOTsink engagement server is not inline, and non-disruptively sits off the trunk port of a switch. The engagement server projects decoys based on unused IP addresses, facilitating fast and frictionless deployment. Since the platform is also self- healing, it will automatically rebuild engagement servers after an attack. This provides easy implementation and eliminates the need for manual rebuilds or maintenance. The ThreatDefend platform has been globally deployed and is in active use amongst many Fortune 500 customers who have validated its ability to scale and effectiveness in large deployments.

STRENGTHENING ENDPOINT DEFENSE

ThreatStrike™ deceptive credentials can be placed throughout the network on endpoint and server devices for credential theft detection, deceiving the attacker into believing that he is harvesting valuable user credentials. Instead, the attacker's use of a stolen credential will have served only to lead him into a deception trap within the BOTsink engagement server. ThreatStrike deceptive credential deployment and operational management is simple given the solution is agentless, does not require endpoint software updates or device-level software, and is easily scalable and customizable, even for large global deployments. Deception credentials include remote access credentials (RDP/SSH/TELNET/VPN), file-server credentials (FTP/SMB/CIFS), mapped shares, and application credentials (Browser-stored/Cookies/Email/ SVN) as rich and attractive attacker targets.

Financial institutions can also use the ThreatDefend platform to guard against attacks on SWIFT financial messaging software by creating ThreatStrike SWIFT credentials pointing to engagement servers with SWIFT-based content and by luring attackers to decoy SWIFT servers. The financial organization can opt to install SWIFT software onto the ThreatDefend platform's engagement servers, to import an image with SWIFT software into the platform's BOTsink solution, to load the SWIFT web page front-end onto the deception engagement server's web service, or to

> Analysts can use the threat intelligence dashboard to drill down into specific threat detail and clickto-activate blocking and quarantine actions driven by integrated 3rd-party solutions.

use the included default SWIFT front-end web page template. These engagement servers can be named in attractive ways that suggest they are true SWIFT servers, not decoys. The ThreatDefend platform can monitor the decoys, providing timely alerts for any attempt to load SWIFT malware or send fraudulent SWIFT messages. The ThreatDefend platform also captures message contents to identify the destination accounts used for fraud.

Endpoint-focused deception provides a way to guard against APT groups by detecting attacker lateral movement early in the attack cycle. Attivo blankets the environment with deceptive credentials to engage attackers as they progress. Unknown to the threat actor, stealing and reusing a deceptive credential triggers an alert and activates forensic collection at the source, providing incident responders the situational awareness they need to prevent an incident from escalating into a business crisis.

EXTENDING THE PERIMETER

For efficient detection for remote offices or branch offices that are small, but still need internal threat detection capabilities, the ThreatDirect™ solution provides deception-based monitoring and detection by forwarding threat activity detected at the remote office to the BOTsink appliance. The solution removes the need for local hardware or devices for local IT staff to maintain.

> The ThreatDefend platform has been globally deployed and is in active use amongst many Fortune 500 customers who have validated its ability to scale.

Support for cloud detection extends to AWS, Azure, VMware, Google, and OpenStack environments, allowing organizations to deploy deception within their private, public, and hybrid data centers.

ATTACK VULNERABILITY ASSESSMENT

Financial organizations can also strengthen their predictive defense by understanding the likely attack paths an attacker would take to penetrate the network. The Attivo ThreatPath solution identifies misconfigurations, exposed, or orphaned credentials that can allow an attacker to spread laterally from one system to another, using the credentials stored on compromised systems. Today's financial institutions can use this visibility into the network to preemptively remediate credential exposures and misconfigurations before an attacker can take advantage of them.

Additionally, such visibility helps to identify routes an attacker would take to target SWIFT systems. Security teams can then remediate these open paths by removing the stored SWIFT credentials or by deploying additional deception assets. The security team can then periodically re-run the assessment to identify new paths that have opened for them to remediate.

STREAMLINE INCIDENT RESPONSE

For streamlined incident response, financial institutions can deploy the Attivo ThreatOps™ solution to build and automate threat defense playbooks. These playbooks are based on integrations with existing security infrastructure and create automated and repeatable incident handling processes. With integrated solutions that enable network quarantine, network access control, endpoint isolation, or threat hunting, the playbooks can automate an incident response action from start to finish. Additionally, because the ThreatDefend Platform has an API available, security teams can access functions from their existing tools, increasing security operations efficiency. By leveraging these automations, organizations reduce the time-to-respond to critical incidents and make it easier for less skilled staff to leverage a playbook to respond to an incident quickly.

COMPLIANCE AND RED TEAM TESTING

It is vital for financial institutions to prove that they meet compliance standards and that their security controls are working reliably. Deception plays a vital role in this process because it can validate network resiliency with early attack detection and by tracking a Red Team's movement during their testing. Attivo Networks has an exceptional track record of catching testers, with examples of teams unknowingly being tracked by the deception environment for periods ranging from hours to weeks.

> With the Attivo Networks ThreatDefend solution, organizations now equip their security teams with powerful detection designed for the volatile and evolving nature of cybersecurity threats.

In addition to slowing the "attacker", the platform acquired and recorded detailed intelligence on the attack. Like what would occur in a real attack, the attacker's progression would have stalled and caused an increase in their time commitment (and therefore costs) as they would be forced to start over once detected or move on to a less difficult target.

WHAT MAKES ATTIVO DECEPTION UNIQUE

Today's financial institutions require an adaptive defense with real-time visibility and in-network threat detection to proactively protect critical financial assets, especially their SWIFT infrastructure. The ThreatDefend™ Deception and Response Platform provides financial organizations the most comprehensive, flexible, and scalable solution to promptly detect and respond to threats that have bypassed other security controls and are inside the network. Deception plays a critical role in empowering an active defense with early threat detection, high-fidelity alerts,

automated attack and vulnerability assessments, attack forensic analysis, and other capabilities that significantly accelerate incident response.

With the Attivo Networks ThreatDefend solution, organizations now equip their security teams with powerful detection designed for the volatile and evolving nature of cybersecurity threats. Moreover, the detailed attack forensics and automated integrations included in platform not only simplifies incident response but also provides on-demand, detailed attack reporting for compliance, pen testing, or other investigative reporting requirements.

For more information about Attivo Networks deception solutions, visit www.attivonetworks.com/solutions/financial/

ABOUT ATTIVO NETWORKS

Attivo Networks® is the leader in dynamic deception technology for real-time detection, analysis, and accelerated response to advanced, credential, Active Directory, insider, and ransomware cyber-attacks. The Attivo ThreatDefend Deception and Response Platform accurately detects advanced in-network threats and provides scalable continuous threat management for user networks, data centers, cloud, IoT, ICS-SCADA, and POS environments.

www.attivonetworks.com

[1] https://www.reuters.com/article/us-cyber-heist-swift-specialreport/special-report-cyber-thieves-exploit-banks-faith-in-swift-transfer-network-idUSKCN0YB0DD

[2] https://www.bankinfosecurity.com/bangladeshi-bank-hackers-steal-100m-a-8958

[3] https://www.reuters.com/article/us-usa-cyber-swift-exclusive/exclusive-swift-confirms-new-cyber-thefts-hacking-tactics-idUSKBN1412NT

[4] https://www.reuters.com/article/us-far-eastern-fine/taiwans-far-eastern-international-fined-t8-million-over-swift-hacking-incident-idUSKBN1E60Y3