Attivo NETWORKS®

Deception Technology for Financial Institutions

Cyberattacks continue to build in volume and complexity with many of the most advanced strains targeted at financial institutions. Despite highly advanced security infrastructure, financial institutions suffer from malicious threat actors and insiders that are able to evade even the most advanced preventions systems. As organizations work to detect and respond to a high volume of suspicious incidents, they are burdened with a considerable drain on resources.

Financial institutions are data-rich and, based on the value of their assets, will continue to remain in the spotlight as primary targets for attackers. Additionally, with each new technology added to the handling, transfer, and storage of critical financial information, new points of entry for attackers are introduced, which inadvertently increase the risk of a breach.

This paper will explore cybersecurity challenges faced by financial organizations and how deception technology can change the game on attackers with reliable in-network threat detection and response capabilities.

Deception Technology for Financial Institutions

Overview

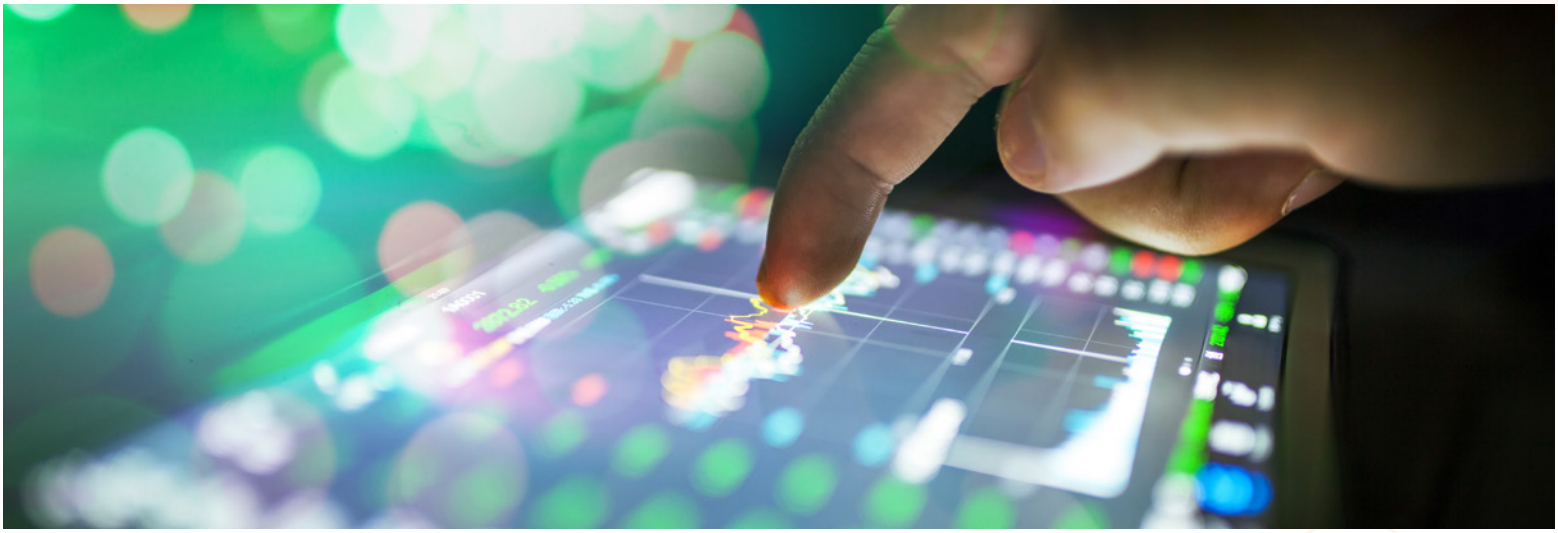
Despite regulations that require financial organizations to adhere to strict cybersecurity measures and strict compliance and security rules, many reputable financial institutions were hit by significant breaches in 2016[1] and many organizations still struggle to reliably pass their required penetration test audits.

Advanced threats have demonstrated that they can and will bypass traditional perimeter security solutions. This means that financial organizations must continue to up their game against advanced attackers. Many organizations have taken steps to embrace an adaptive defense that includes prevention, detection, response, and attack predictability, however even that is not proving to be enough. Attackers are continuing to advance their sophistication and techniques they use to avoid detection and complete attacks, yielding in unprecedented levels of financial data theft.

One of the greatest challenges faced by computer security professionals is the inability to detect early credential theft and lateral movement within their computer systems or networks, reflecting an overreliance on their perimeter defenses. This failing is why attackers are able to remain undetected for extended periods of time and disappear into the litany of alerts practitioners receive. Due to this crucial issue, a 2016 Ponemon Institute study found that organizations on average took more than six months to identify a security breach, as well as an additional 66 days to contain the breach after discovery. This lack of detection resulted in 1,935 successful breaches in 2016, according to the Verizon DBIR report.

This paper reviews the challenges that financial institutions face in protecting environments from information security attacks and how new deception technology can be applied to close security gaps and further strengthen their security defenses. Deception-based detection technology changes the game on attackers; taking a page out of military operations, Attivo applies deception-based decoy and attacker luring technologies within the network to deceive and misdirect attackers into revealing themselves. It presents a unique opportunity to change the asymmetry of war against cyber attackers, altering their reality and imposing increased cost as they are forced to decipher what is real and what is fake. To retain control, financial organizations must exploit the trust that attackers have in order to reduce the noise and turn the tide against them.

...a 2016 Ponemon Institute study found that organizations on average took more than six months to identify a security breach, as well as an additional 66 days to contain the breach after discovery.



Challenges

Financial institutions are renowned for having invested in and having access to the most advanced security infrastructure. Yet despite substantial investments, there continue to be gaps in security controls or human error that impedes the consistent, reliable, and early detection of breaches. The security sophistication of a financial organization also comes with heavy operational overhead. There are considerable operational and staffing costs required to keep up with the masses of alerts and threat information logs, all at a time when there is an unprecedented lack of skilled workers. Early threat detection is needed more than ever, as is the ability to do this efficiently and accurately.

Regulatory

Governmental rules and compliance standards, intended to ensure that a breach does not happen, can inadvertently limit an organization's ability to take effective breach prevention actions, particularly in the difficult task of regulatory compliance across borders.

Regulations meant to create a more protective environment can impair the ability to effectively fight and react to threats. For instance, the New York Department of Financial Services' (DFS) Cybersecurity Regulations, entered into effect on March 1st, 2017 and under the regulations, financial organizations are required to assess their security posture and "establish and maintain a cybersecurity program designed to address such risks in a 'robust' fashion"[2]. What is particularly onerous to organizations about regulations like this is the documentation required to prove that a cybersecurity program meeting the qualifications is maintained. By diverting resources to keep extensive documentation, already taxed security teams are burdened with compliance red tape and pulled from focusing on the threats themselves.

Yet another example is the General Data Protection Regulation (GDPR). The GDPR seeks to consolidate and strengthen data protection rules for individuals living in the European Union (EU). For organizations, however, this regulation applies to all entities that market goods or services in the EU, regardless of whether the data is collected, stored, or processed outside of the EU.

With strict privacy rules, come strict disclosure rules. Under the GDPR, organizations must disclose of a breach within 72 hours of learning of the incident and "must provide specific details of the breach such as nature of it and the approximate number of data subjects affected"[3]. The daunting aspect of this rule is that it takes organization in the EMEA region an average of 469 days to discover a breach in their network. With the alarming time it takes organizations to discover breaches, disclosing them to the public with comprehensive details can be extremely difficult and result in significant public backlash.

With today's use of the Internet in a cloud connected world, borders are not always physical. Managing security compliance across virtual company borders presents its own set of challenges. Partnerships, outsourcing, and offshoring present unique threats to information security because financial organizations have little control over the security measures of other companies and are often unclear on where data actually resides. Further, processes implemented to manage partnerships and providers often lack visibility into security measures. This can lead to security gaps, particularly during periods of transition, that are difficult to identify and remediate.

Managing compliance is required, but the far greater challenge is for financial institutions to combat the constantly changing attack surface and a growing reliance on suppliers and partners, which are often the weakest link. It is a never-ending-battle.

Malware

AV-TEST reports that 120 million new strains of malware were introduced in 2016 alone.[4] For signature-based security devices rooted in detecting known attack patterns, addressing the 328,000 new pieces of malware created every day can be draining. In addition to that, zero day and targeted attacks can make the situation appear overwhelming.

The Dridex banking Trojan is amongst the most feared malware and it has been said that the moneymakers behind Dridex are successfully infecting thousands of users worldwide on a monthly basis. The example of Dridex is typical of many different types of malware and represents the uphill battle facing financial organizations in attempting to defend their critical data from attackers. It is a strain of malware originally written to attack European banks, but has morphed to plague several different types of financial institutions around the globe.

> *With the alarming time it takes organizations to discover breaches, disclosing them to the public with comprehensive details can be extremely difficult and result in significant public backlash.*

Dridex works by leveraging macros in Microsoft Office to infect systems and, once successful, steals banking credentials and other administrative information to gain access to financial records[5]. This malware can carry many different types of payloads, including ransomware. Once ransomware gets into a system, it encrypts data files and demands money in exchange for decryption. Unchecked ransomware can infect an entire network, resulting in ransom demands that have been reported as high as one million dollars or 397 Bitcoin[6].

What makes Dridex particularly dangerous are the estimated thousands of mutations of the malware in the cyber security ecosystem. Each has a unique signature and many are essentially the same version. Additionally, with a few minor changes between mutations, each is designed to generate unique signatures. Each time a mutation is identified by the security devices of an organization, the attacker retires it and prepares a new one to be released in the next attack.

Thousands of iterations, ever multiplying and mutating, overwhelm the ability of conventional prevention devices to stop Dridex malware from penetrating the network. Once inside the network, the malware can freely move laterally between systems by blending in with "normal" traffic and take months harvesting credentials to escalate their attack.

Application level security

The Security Score card 2016 Financial Industry Cyber Security Report says that many financial organizations still fail at application level security. Potential vulnerabilities at the application level allow attackers to drop SQL or code injection into a web shell with their own script, which goes undetected by traditional prevention security devices. The undetected script can be used by an attacker to run advanced reconnaissance missions throughout the network, allowing the attacker to identify targets for credential exploitation or infection. These stealth missions are essential to the attack kill chain and tend to go unnoticed by most security controls or get lost in security logs.

Neglected security updates and unpatched systems create backdoors for preventable malware to infiltrate systems and move laterally through the network, often undetected until after they have compromised critical assets. This situation is compounded as financial institutions continually move toward a 24/7 service model of availability with little downtime left to do security updates and software patching. Individual user behavior also continues to challenge organizations as employees delay upgrades or fall prey to attacker phishing emails or Man-in-the-Middle types of attacks[7].

It is critical for financial institutions to have both end-point, Active Directory, and network level detection to be able to detect credential-based attacks and the lateral movement of attackers as they seek to escalate attacks. Ideally, the financial organization detects the attacker the instant a credential is compromised or as early reconnaissance is conducted. Early visibility into suspicious lateral movements can thwart an attacker's efforts before the attack has the opportunity to harvest the credentials they need. Additionally, insight into misconfigured, exposed, and orphaned credentials provides knowledge of where vulnerabilities exist and the attack paths an attacker would take to reach their target assets.

Unchecked ransomware can infect an entire network, resulting in ransom demands that have been reported as high as one million dollars or 397 Bitcoin

Resource Drain

Another significant challenge that financial institutions face is the eminent shortage of cybersecurity workers. Reports estimate that the cybersecurity industry will have a deficit of 1.8 million employees by 2022[8]. In addition to a crippling shortage of personnel, organizations are consistently confronted with a shortage of skills. The future outlook is also not promising, as the majority of organizations report that less than a quarter of applicants for open cybersecurity positions possess the basic requirements for the position[9].

While the personnel and skills shortage affect all types of organizations, financial organizations are thrown into a particularly precarious situation. Because of the highly-regulated nature of banks, they cannot afford to suffer any breach that threatens the financial information of their customers[10]. Furthermore, to attract the talent they need, financial institutions are forced to pay the highest salaries to security workers, more than any other type of organization, meaning that institutions are paying more money for less personnel and less talent[11].

Deception technology

With a new approach needed, financial organizations are turning to deception technology to change the asymmetry on attackers. Some are first time deception technology adopters that are drawn to the accuracy and efficiency of the solution and others are migrating off home grown honeypot technology for the additional accuracy and operational efficiency. Deception technology works by turning the network into a trap with a maze of misdirection that will trick an attacker into engaging and revealing their presence. In a deception network, the attacker need make only one small engagement mistake and their presence will be known. By being present at the network layer and end-point, deception technology significantly increases the likelihood that an attacker will inadvertently engage with a deception system during reconnaissance or while harvesting credentials. Deception also addresses alert and log fatigue because it will only generate an alert upon actual attacker engagement. Each alert is substantiated and includes the details of the attacker actions, movement, and attempted use of deception credentials. Automation can also be applied through endpoint, firewall, and NAC integrations to isolate the infected system in preparation for remediation.

The deception platform, posing as an attractive target, lures the attacker into engaging. The platform analyzes each attack, capturing the attacker's valuable Tactics, Techniques, and Procedures (TTPs) to block the attack and better fortify the network in the future. This information can then be manually or automatically applied to prevention and other detection systems, automating incident response and making overall defenses stronger via shared attack information.

This Dridex malware example shows how deception can be applied for early detection and response to an attack. There are three stages of the Dridex attack chain that leverage the detection gaps inherent in traditional security devices. This is where deception plays a valuable role in closing the detection gap:

1. **Internal Reconnaissance** – The attacker conducts internal network reconnaissance to identify high-value assets or assets with digital proximity to assets that store financial data. Internal reconnaissance actions by the attacker go undetected because they are conducted over a period of weeks or months and therefore blend in with the "normal" traffic on the network. Deception decoys can be strategically placed to appear as production assets and deception lures are planted to attract attackers into engaging. Any attempt by an attacker to conduct reconnaissance or scan a network, a deceptive asset will signal malicious intent and trigger an alarm.

2. **Lateral Movement and Credential Harvesting** – After identifying key locations or credential targets, attackers will further attack goals. The attacker then moves to those locations to execute its objectives. To do so, the attacker must harvest credentials that allow such movements. 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, etc.
    b. Performing Man-in-the-Middle attacks to intercept credentials in transit.

After harvesting legitimate administrative credentials from an endpoint, the attacker can move freely and undetected throughout the network. Because the intruder uses legitimate credentials, it is extremely difficult for most traditional security devices to detect the attacker.

Deception systems, however, can play an important role by feeding misinformation to the attacker that seeks to steal credentials. Deception platforms place attractive deception credentials on an endpoint or server with the goal to entice the attacker to steal false credentials that appear as ones of a legitimate user or a network shared drive. The moment an attacker attempts to use the deception credential, they are led to a deception server where the platform raises an alert, reveals the presence of the attacker, conducts an analysis of the attack, and studies for polymorphic activity. Communications with Command and Control (C&C) systems can be safely opened to gain added insight into the attacker's tools, methods, and attempts to implement commands.

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

Without deception, the detection of 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 or sharing of a malicious file) to those activated at the database tier (from an exploited web application) to man-in-the-middle attacks, deceptive assets maximize protection by luring attackers at all levels of the network.

Deception platforms can also provide automated attack analysis, forensic reporting capabilities, and automations for incident response (blocking, quarantine, threat hunting). This can save time and resources associated with understanding the attack, correlating attack information, producing forensic reporting for attack documentation, and incident handling. Thus, the deception platform significantly reduces time-to-detection, providing the context organizations need for remediating an attack before it can cause damage to the network.

Deception platforms place attractive deception credentials on an endpoint or server with the goal to entice the attacker to steal false credentials that appear as ones of a legitimate user or a network shared drive.

3. **Exfiltration** – It is critical for an organization to stop an attacker from exporting sensitive financial or company data from a network. Deception platforms provide valuable insight that cannot be gathered by tools that only block or stop at merely detecting an attack. With the ability to gather information about the attack's payload, its activities, and communications from Command and Control (C&C), deception platforms can not only detect, but also collect, analyze, and report on attacks in order to block 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 at the perimeter, preventing data exfiltration. The solution can also be instrumental during polymorphic attacks since it will continue to update signatures generated over time based upon additional time triggered C&C communications.

The Attivo Solution for Deception-based Detection and Response

Attivo Networks is consistently recognized for its innovation and leadership in deception-based information security defense. The company's heritage and leadership resides 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, and POS.

Offering the most 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 to:

- Set highly authentic and interactive traps and lures to detect threats from human (advanced persistent threat [APT], insiders, third 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 attacks
- Provide visibility into insider, contractor and supplier third-party threats as they conduct reconnaissance and move laterally through networks.
- Detect zero-day and advanced threats with no dependency on signatures, known attack patterns, or database queries.
- Bolster endpoint defense with agentless deceptions designed to plant credential and ransomware lures.
- Scale and provide operationally efficient deployments for large global networks
- Flexible deployment in appliance, VM, or cloud configurations, modular design facilitates seamless expansion of new functionality
- Deliver only high-fidelity, real-time alerts triggered by the detection and engagement of an attacker.
- Provide a threat intelligence dashboard for a centralized view of all alerts and actionable drill down for simplified incident response.
- Attack Threat Analysis engine for automating attack correlation and generating forensic reports
- Accelerate incident response (block, quarantine, threat hunt) through 3rd party integrations with firewall, NAC, end-point, and SIEM vendors.
- Create repeatable incident response playbooks using the ThreatOps module.
- Identify and graphically show misconfigured, misused, orphaned credentials to shut down attack path vulnerabilities.
- Show attack time-lapsed replay for understanding attacks and strengthening defenses.

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 platform, based on its Camouflage Deception techniques and Adaptive Deception Campaigns, attracts the attacker by running real operating systems and golden images of production asset software. These capabilities are used to fool attackers by causing decoy engagement servers to become indistinguishable from production assets, luring attackers away from assets that must be protected.

Additionally, the solution uses machine learning to create Adaptive Deception Campaigns, which propose new deception campaigns and enable credentials and decoys to be automatically refreshed based on time or suspicion of an attack that may be underway. Additionally, decoys can be automatically set to not only rebuild, but respin after attacker engagement to avoid fingerprinting.

Automated Attack Analysis and Response

Responding to an incident does not stop with detection. The Attivo solution goes one step further and provides the tools required for prompt incident handling and response. All alerts are evidence-based with the substantiated, actionable detail required to identify the infected device and understand the attacker's actions. The attacker's IP, tools, and methods can be obtained if communications with Command and Control are established. Because alerts reveal attack details, incident handling for security analysts is improved as they can now quickly and confidently quarantine a device and remediate an attack. The Attivo Attack Threat Analysis (ATA) tool will track and record the attacker's actions for forensic evidence reporting. The Attivo Malware Analysis Sandbox (MAS) also provides in-depth analysis of malware and phishing emails, removing hours of time that would traditionally be dedicated to testing binary files.

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. IOC, PCAP, STIX, CSV, and other reporting formats can be created to easily share attack information detail. Third-party integration with SIEM solutions like Splunk, ArcSight, and QRadar are provided along with the integration of popular firewalls, NAC, and endpoint software to automatically block, quarantine, and remediate infected devices. Additional integration, with companies like CarbonBlack, ForeScout, and McAfee ePO, supports the transfer of attack information, facilitating the hunt and eradication of threats from the network.

Counterintelligence

In addition to understanding what and how the attacker attacked, it becomes increasingly valuable to understand what they are looking for and where the information is ending up. Attivo data deceptions include a tracking mechanism to understand where a file ends up and also empowers the organization with the ability to plant fake documents. These documents can be used to create doubt as to the integrity of what was stolen, which will slow an attacker and increase their costs as they now need to validate the integrity of what was stolen.

Scalability

Deployment of the ThreatDefend platform is, by design, highly scalable. The BOTsink engagement server is not online 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 for easy deployment and eliminates the need for manual rebuilds or maintenance. The ThreatDefend platform has been globally deployed and is in active use amongst many Fortune customers who have validated its ability to scale and be effective in large scale deployments.

Deployment and operational management of ThreatStrike deceptive credentials is simple given the solution is agentless, does not require updates of endpoint software or device-level software, and is easily scalable and customizable, even for large global 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. Deployment and operational management of ThreatStrike deceptive credentials is simple given the solution is agentless, does not require updates of endpoint software 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 deception technology 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 deception platform's engagement servers, to import an image with SWIFT software into the platform's BOTsink solution or to load the SWIFT web page front-end onto the deception engagement server's web service. These engagement servers can be named in attractive ways that suggest they are true SWIFT servers, not decoys. The decoys can be monitored, providing timely alerts of any attempt by attackers to load SWIFT malware or send fraudulent SWIFT messages. The deception platform also captures message contents to identify the destination accounts used for fraud.

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.

Support for cloud detection extends to AWS, Azure, VMware, 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 and exposed and orphaned credentials that can allow an attacker to spread laterally from one system to another, using the stored credentials of those compromised systems. Today's financial institution can use this visibility into the network to preemptively remediate credential exposures and misconfigurations before any attacker can take advantage of them.

Attivo Networks has an exceptional track record of catching pen testers with examples expanding from hours to weeks that the tester was distracted within the deception environment.

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 upon integrations with existing security infrastructure and create automated and repeatable incident handling processes. This not only reduces the time-to-respond to critical incidents, but also makes it easier for less skilled staff to leverage a playbook to quickly respond to an incident.

Compliance and Red Team Testing

Proving that compliance standards are met and that security controls are working reliably is critical. Deception plays an important 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 pen testers with examples expanding from hours to weeks that the tester was distracted within the deception environment. In addition to slowing the attack, attacker intel was acquired and recorded. In the event of this being a real attack, the attacker would have experienced delays in their attack and an increase in the cost as they would be forced to start over once detected or move on to a less difficult target.

Conclusion

Today's financial institutions require an adaptive defense with real-time visibility and in-network threat detection to proactively protect financial data from exfiltration or compromised access to data. The ThreatDefend Deception and Response Platform provides financial organizations the most comprehensive and scalable solution to promptly detect and respond to threats that have bypassed their security controls and are inside the network. Deception plays a critical role in empowering an adaptive defense with early threat detection, automated attack and vulnerability assessments, attack forensic analysis, and other capabilities that significantly accelerate incident response.

With the Attivo Networks comprehensive deception platform, organizations equip their security team with powerful detection designed for the volatile and evolving nature of cybersecurity threats. Moreover, the detailed attack forensics and automating integrations included in the ThreatDefend Platform simplify incident response and provide on-demand detailed attack reporting for compliance, pen testing, or other investigating reporting requirements.

For more information about Attivo Networks deception solutions, visit https://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

References:

1) https://cdn2.hubspot.net/hubfs/533449/SecurityScorecard_2016_Financial_Report.pdf
2) https://corpgov.law.harvard.edu/2017/03/25/new-york-cybersecurity-regulations-for-financial-institutions-enter-into-effect/
3) https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection
4) https://www.av-test.org/en/statistics/malware/
5) http://www.webopedia.com/TERM/D/dridex-malware.html
6) https://www.cnet.com/news/largest-ransomware-ever-demand-south-korea-web-host/
7) https://www.infosecurity-magazine.com/news-features/almost-a-third-of-staff-fall-for/
8) http://www.bizjournals.com/stlouis/news/2017/03/27/with-shortage-of-cybersecurity-workers.html
9) http://thehill.com/blogs/congress-blog/technology/239113-cybersecurity-talent-worse-than-a-skills-shortage-its-a
10) http://sponsoredcontent.wsj.com/pwc/broader-perspectives/cyber-matters-skills-shortage-will-force-cybersecurity-rethink/
11) http://sponsoredcontent.wsj.com/pwc/broader-perspectives/cyber-matters-skills-shortage-will-force-cybersecurity-rethink/