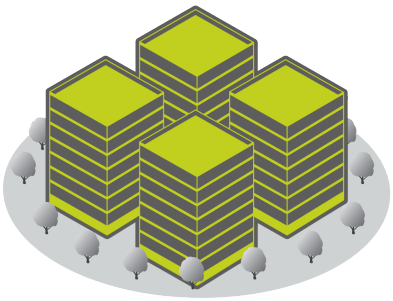
[secure]®

ISC8

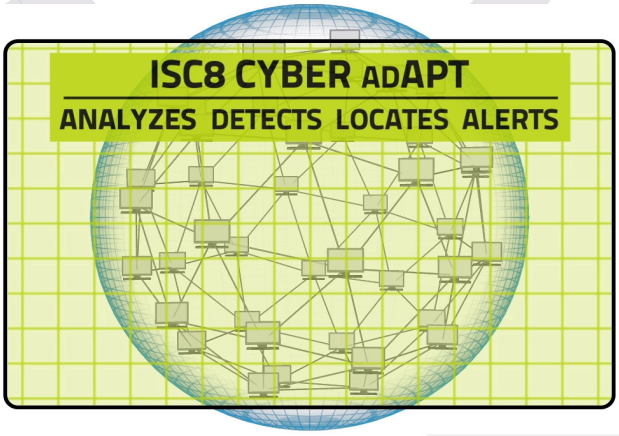


Banking and Finance

Financial Institutions are Second only to the Department of Defense in Targeted Cyber Attacks

Advanced malware that evades signature-based detection has increased by almost 400 percent since 2011

- The number of these advanced malware attacks is increasing at a steady rate while also growing more sophisticated and complex. Attackers don't rely solely on penetrating a firewall or Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS) to gain access to the network.
- Social engineering campaigns like "spear phishing" are used to coerce users to open the front door and expose your network. PDF files and images which are already unknowingly infected are regularly downloaded by users and employees, providing an open door into your network core.



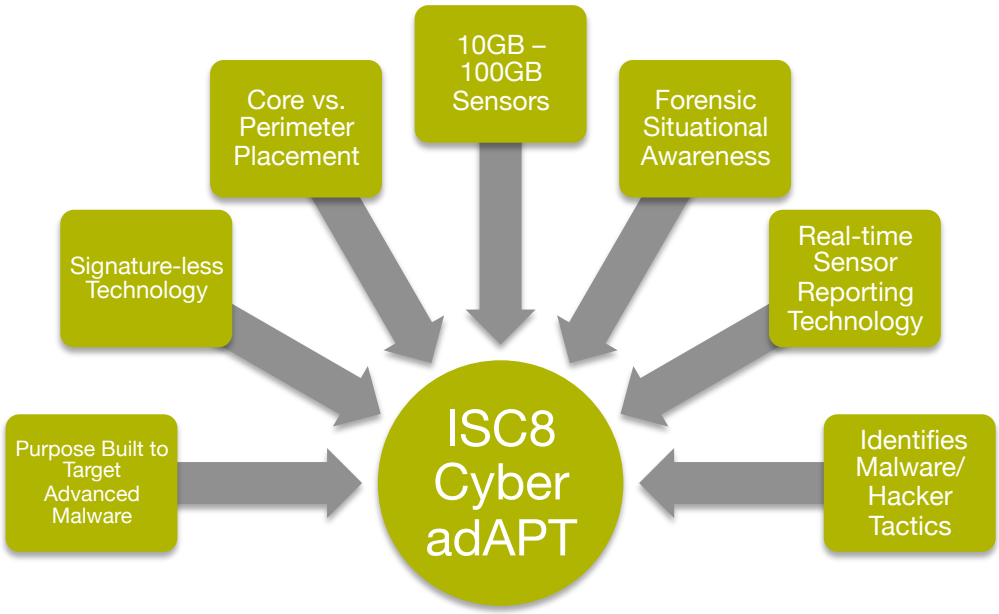
Cybersecurity Solutions for the Financial Services Industry

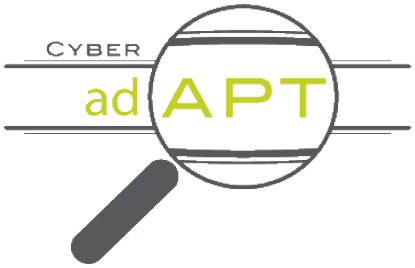
PROTECTION FROM EVOLVING, SOPHISTICATED THREATS

- Recently, banks have been disrupted by sophisticated hackers causing a series of ***distributed denial-of-service*** (DDoS) attacks worldwide. ***These attackers are changing their signatures every 7-10 seconds***, rendering signature-based defenses ineffective. The real threat may be in what they leave behind
- FS-ISAC (**Financial Services Information Sharing and Analysis Center)** for the first time raised its cyberthreat level to "high,"
- CISO Strategy from a leading bank; "We must keep identifying the new threats and finding the right solution to mitigate the risks." from *BankInfoSecurity*

[secure]®
ISC8

Banking and Finance





ISC8 Cyber adAPT : Signature-less, Advanced Threat Detection

The Next Generation in Cybersecurity… Automated, Real-time, High Speed, Forensic Analysis

Todays Advanced Malware Are Sophisticated

APTs attacking banks and financial organizations now employ a variety of techniques to breach the "secure" perimeter of the enterprise. Once inside, APTs are designed to stay invisible and propagate from one host to another, establish Command and Control and successfully extract proprietary and confidential data. These programs often cloak their actions as legitimate, benign network activity ensuring the threat goes unnoticed by legacy anti-malware solutions.

Compelling new cybersecurity solutions from ISC8 offer many benefits to financial institutions:

- Automated threat analysis
- Improved operational efficiency
- Stronger security posture
- Speedy threat response

Real-time, advanced threat detection.

- **Alerts** to suspicious behaviors before they can do severe damage, breaching critical data and harming your reputation.
- **Analyzes** signs of malware behavior correlated over long periods of time, detecting new and emerging malware in near real time.
- **Does not rely** on vendor signatures but analyzes real zero day attack methods to keep false positives low

Signature-based solutions are rendered useless against today's complex eco-system of cyber threats. As quickly as vendors identify and deploy a signature for a particular exploit, malware code writers are modifying and adapting their code to ensure the exploit is still viable.

Attackers are already in your network. They've been there for months… maybe years. How do you detect, disarm and dispose of them before they cause severe harm?

www.ISC8.com CyberSecurity@isc8.com