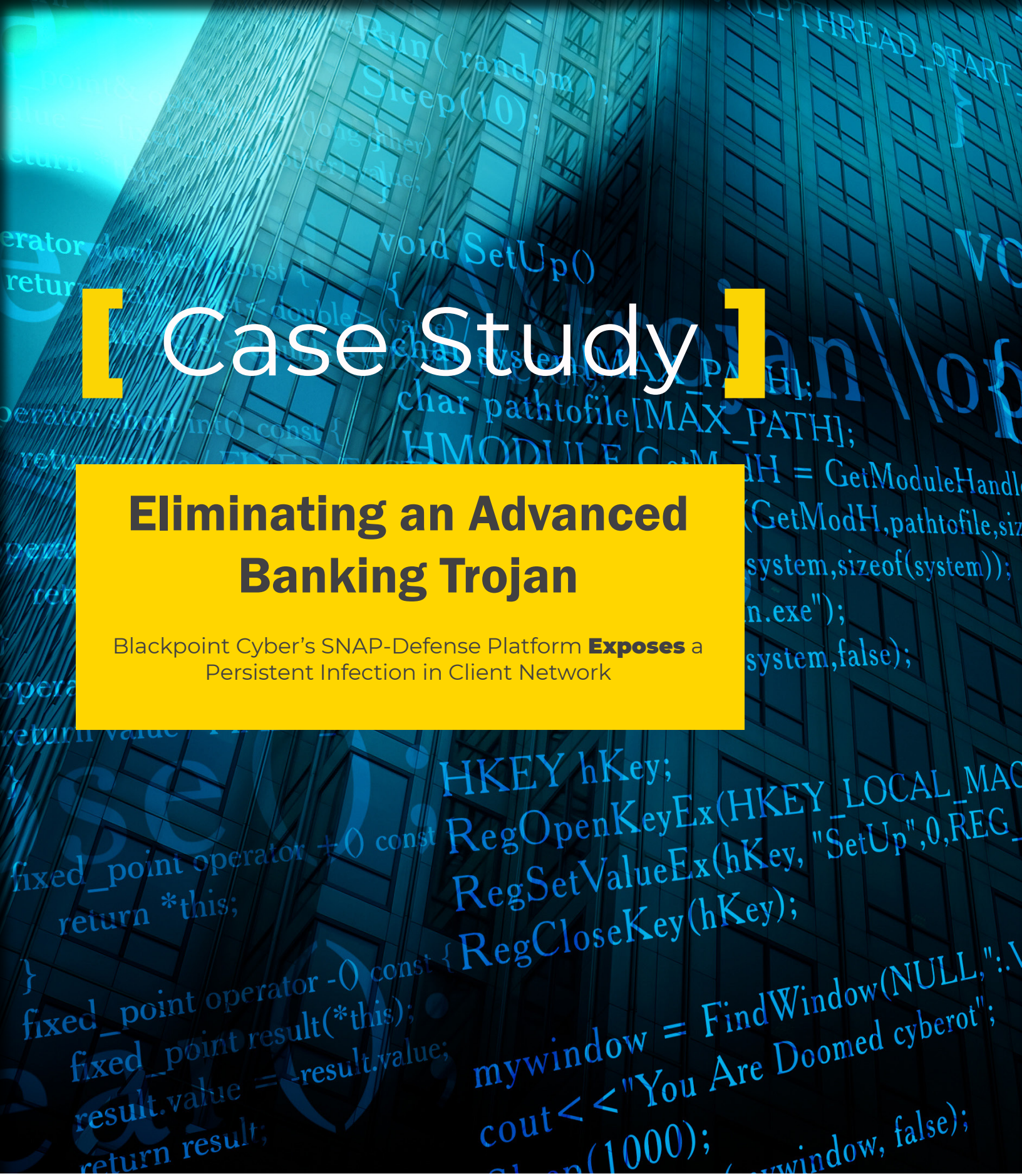


Case Study

Eliminating an Advanced Banking Trojan

Blackpoint Cyber's SNAP-Defense Platform **Exposes** a Persistent Infection in Client Network

blackpoint

The Client

Powerful Managed Service Provider

CoreRecon is a cyber security and IT services company with over 30 years of experience. The company provides advanced IT and cyber security solutions to their clients, securing enterprises against sophisticated, living-off-the-land cyber-attacks by leveraging Blackpoint's patented security operations and incident response platform: SNAP-Defense.

The Challenge

An Unknown Threat Disrupting Business Operations

A client approached CoreRecon with complaints about their IT infrastructure; the employees were having to frequently re-boot their PCs and experiencing other day-to-day issues. The client revealed that their internal IT staff was tasked with identifying and resolving the issue. Although the IT staff purchased various premium products to find the root cause, they eventually abandoned the project since none of the tools helped identify or resolve the issue. Without visibility and awareness of privileged user and lateral spread activity, the IT staff was unable to detect the serious, advanced trojan ripping through their network.

Employing SNAP-Defense

Previous to this incident, CoreRecon's IT and security staff investigated many offerings in a search for real-time visibility into their clients' networks, better monitoring of privileged user activity, alerting of dangerous lateral spread activity, and an advanced cyber security operations platform with integrated anti-malware. After an in-depth analysis of various options, CoreRecon chose SNAP-Defense as the foundation for its continuous cyber security monitoring services and now requires all its clients to deploy Blackpoint's SNAP-Defense platform and advanced anti-malware technology.

Origin of SNAP-Defense

Blackpoint built SNAP-Defense after years of experience conducting real-world cyber security operations for United States Government intelligence agencies. Blackpoint's senior leadership used their first-hand knowledge of how attackers gain access, abuse, and move through a victim's network and analyzed real-world cyber-attacks to build patented technology that identifies cyber-attack threats faster and better than traditional cyber security products.

The new client's situation presented a perfect opportunity to test out the advanced capabilities of Blackpoint's offerings. So CoreRecon deployed SNAP-Defense and the advanced anti-malware technology to discover what exactly was occurring in the concerned client's network.

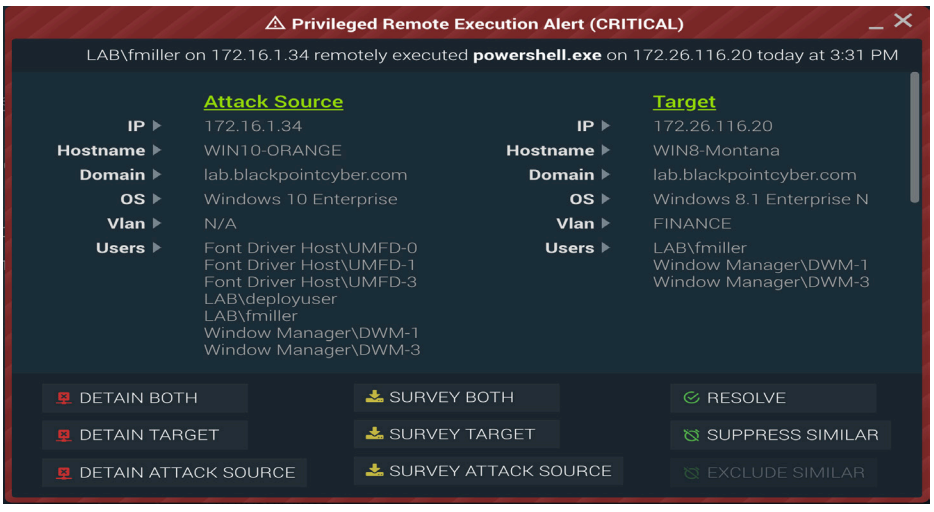
Eliminating the Infection

1. CoreRecon deployed the SNAP-Defense and anti-malware agents to the client's IT infrastructure in a matter of minutes

2. SNAP-Defense immediately created a real-time network map, giving CoreRecon complete visibility into the compromised network

3. The SNAP-Defense platform began showing real-time threat alerts with data from the integrated anti-malware technology

4. Using SNAP-Defense and the anti-malware technology, CoreRecon started cleaning infected devices while monitoring for new threats



5. Once the infrastructure was cleaned, CoreRecon continued monitoring the client's network with SNAP-Defense to prevent future attacks

The Results

Client's Network Cleaned and Secure

VISIBILITY

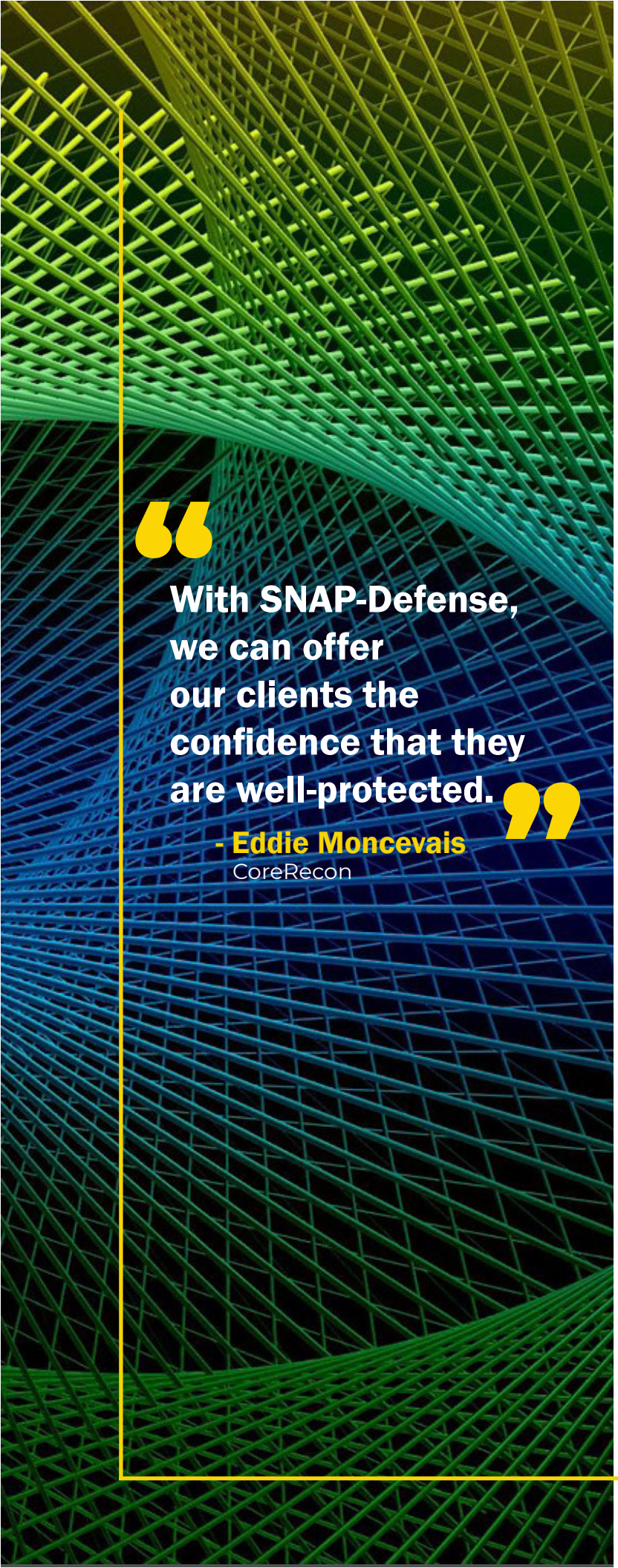
Immediately after deployment, SNAP-Defense mapped the client's network, providing CoreRecon with a map of connected devices and users

DETECTION

Within minutes of deployment, SNAP-Defense identified compromised devices, where they were located, and the spreading infection activity occurring on each device

RESPONSE

Within a few days, the entire network was infection free thanks to CoreRecon, Blackpoint's SNAP-Defense, and the anti-malware technology



blackpoint

Cyber-attacks are constantly evolving; companies need to invest in services and technologies that keep them ahead of attackers. SNAP-Defense is that technology, enabling Managed Service Providers like CoreRecon to provide effective continuous security services by leveraging real-time visibility in their clients' networks, modern threat detection, and the ability to respond immediately to identified threats.

Contact

Nicole LaDue

Blackpoint Cyber
240.538.7598
nladue@blackpointcyber.com