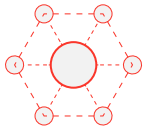
Financial Services - Ransomware

A Use Case Addressing Cyber Crime and Their Targets

NOPSEC

The Problem

Ransomware has become increasingly popular with cybercriminals, and the financial service industry has become one of their favorite targets. There are several contributing factors:

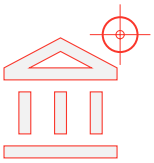


Expanded Attack Surface

The pandemic gave cybercriminals more openings, as the attack surface expanded due to the shift to remote work and the inherent lack of protection of home-based connectivity methods

Ransomware-as-a-Service

Ransomware-as-a-Service has become an offering on the dark web, lowering the technical barriers that previously limited the number of threat actors who could participate in the activity



Financial Institution Targeting

Financial institutions are prime targets because they contain large amounts of personally identifiable information (PII) – the type that no business wants shared publicly – and can be used to shut down the organization's operations until a ransom is paid

RANSOMWARE: THE NUMBEVRS

1,318% the year-on-year increase in ransomware attacks on the banking industry in the first half of 2021[1]

21% percentage of attacks using ransomware, the most popular type in 2021[2]

90% percentage of financial institutions subject to a ransomware attack in 2020

There's little reason to think ransomware will fade as a threat anytime soon. Cybercriminals are earning billions by deploying it. And while law enforcement agencies and others are able to identify and shut down some of the major players exploiting ransomware, the individuals involved often regroup and continue their exploits.

1 "Attacks from All Angles: 2021 Midyear Security Roundup," Trend Micro, Sept. 14, 2021
2 "X-Force Threat Intelligence Index 2022," IBM Security

The Challenge

The fundamental nature of financial services is such that the industry will continue to receive a disproportionate amount of ransomware attacks. Additionally, the larger attack surfaces created during the pandemic are not likely to contract significantly, as working-from-home becomes a permanent option for a significant number of financial services employees. With these elements in place, how do financial institutions limit their exposure to ransomware?

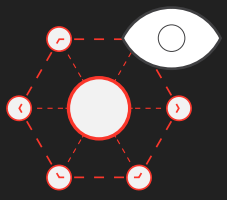
The Solution

While the attack surface may not shrink, it can be better protected. That means first understanding where there are weaknesses, shoring them up, continuously updating the assets that constitute the attack surface, and responding to attacks logically and methodically.

NopSec's Unified VRM gives financial institutions the ability to see all their external-facing assets and systems in one view. Regardless of the department, the database, or the operational/information flow, Unified VRM provides complete visibility and the resultant control it makes possible:

NOPSEC UNIFIED VRM

Monitoring



Continuously observes a variety of hybrid environments externally and distributed ecosystems (such as cloud services and external-facing on-premises infrastructures), including all those potential entry points posed by your remote workforce

Asset Discovery

Discovers and maps unknown external-facing assets and systems to the organization to include shadow IT, unmanaged assets, and internet-facing devices from outside the organization that may be connected to the corporate network

Analysis

Evaluates and analyzes asset attributes to determine if an asset is risky, vulnerable, or behaving abnormally outside of the baseline

Prioritization

Prioritizes risks and vulnerabilities and provides alerts based on prioritization analytics

Remediation

Provides automated action plans on the mitigation of prioritized threats with embedded native detection and response capabilities

NopSec Unified VRM gives financial institutions the attack surface management tools they need to identify vulnerabilities and threats, even when their infrastructure is complex and lacks centralized controls of its own. Using AL/ML, it goes beyond providing alerts to contextualizing them. This means security teams get prioritized lists of issues to address that saves time and effort and speeds response times, lessening potential impacts.

Contact NopSec for a demo today.