Addressing the Critical Threat of ShinyHunters:

How DPRM Can Protect Against Advanced Cyber Attacks

The recent breach hitting a leading financial services company, affecting 30 million individuals, underscores the critical threat posed by sophisticated hacking groups such as ShinyHunters. This attack, part of a worrying trend, highlights the increased targeting of the financial services sector, which holds vast amounts of sensitive data.

Notorious for orchestrating some of the most high-profile data breaches across multiple sectors, ShinyHunters have exploited stolen legitimate credentials to infiltrate cloud services and database infrastructures, collecting and reselling valuable user data for profit. This attack comes recently after their hit on Ticketmaster, with the hackers still trying to sell Ticketmaster stolen data on the internet. Testament to their capabilities, the severe risks they pose, and a further threat to others in data-rich industries, such as the financial sector.

The Gravity of the ShinyHunters attacks

The magnitude of the hackers’ recent breaches cannot be overstated. By leveraging legitimate credentials, ShinyHunters have infiltrated company networks, targeting Active Directory (AD) to create superuser accounts with escalated privileges. The hacker's newsworthy breaches are a stark reminder of how critical it is to safeguard against advanced cyber threats that can gain access and exploit core network infrastructures.

> **“The sophistication and boldness of ShinyHunters highlight a disturbing trend in the cyber threat landscape. This group has a history of targeting major organisations, exploiting vulnerabilities, and stealing vast amounts of data.”**
>
> *Simon Pamplin – CTO, Certes*

The sophistication and boldness of ShinyHunters highlight a disturbing trend in the cyber threat landscape. This group has a history of targeting major organisations, exploiting vulnerabilities, and stealing vast amounts of data. Their methodical approach and ability to evade detection until significant damage is done demonstrates the pressing need for businesses to ensure robust security measures.

ShinyHunters have compromised approximately 770 million records across various attacks so far, generating an estimated $40,000 to $70,000 in monthly revenue from selling stolen data.

The Gravity of the ShinyHunters attacks

With the average cost of a data breach hitting record highs at $4.45 million - Businesses' data security measures need to advance at great lengths to put a stop to threats. The solution: Data Protection and Risk Mitigation - DPRM focuses 100% on protecting your data irrespective of the infrastructure it flows over. Certes DPRM protects you against ransomware and ensures that attempted data breaches are pointless and invaluable to the attacker.

Here’s how DPRM can protect your data:

1. **Advanced and Patented Data Protection**

   Certes DPRM protects data in transit in such a way that it is only readable by the customer and the intended recipient. This ensures that even if data is intercepted or exfiltrated, it remains unreadable to the attacker.

2. **Zero Trust Data Access**

   Our Zero Trust Data Access model ensures that just because someone can access the network doesn’t mean they are approved to access the data. This approach significantly reduces the risk of unauthorised access and credential misuse. With data breaches linked to weak, default, or stolen passwords, this model is crucial for enhancing security.

3. **Crypto-Segmentation**

   At the heart of Certes DPRM's approach is crypto-segmentation. This technology allows for the individual securing of application data flows with unique policies and encryption keys, effectively creating discrete crypto segments that safeguard sensitive data from unauthorised access and lateral movement within a network. This protects against sophisticated methods of moving through a network.

4 Customer-Controlled Key Management

With DPRM, the customer controls all encryption keys, ensuring you are not reliant on your service provider, cloud provider, or vendor's security to protect your data. This ensures that only the customer can control access to the data, providing additional layers of security.

Specific Measures Against Active Directory Compromise

- **Preventing Escalated Privileges:** Certes DPRM employs data-centric segmentation to safeguard AD. Segmenting each data flow with unique policies creates discrete segments that prevent unauthorised access and lateral movement within the network. This ensures that even if an attacker gains initial access, they cannot escalate or manipulate sensitive AD data. Given that 50% of organisations have experienced cyberattacks involving Active Directory compromises in the past two years, this protection is vital.
- **Mitigating Data Exfiltration:** Certes DPRM ensures that data leaving the site is useless to attackers. By applying protection policies controlled solely by the organisation’s security team, any exfiltrated data remains indecipherable.
- **Securing Active Directory Against Advanced Threats:** AD is a prime target for attackers due to its central role in managing user identities and access controls. Compromising AD can provide attackers with broad network access and control. The sensitive nature of the data stored in the NTDS.dit file, including hashed passwords, makes it particularly attractive. Attackers often use tools like Volume Shadow Copy, NTDSUtil, and Mimikatz to extract and exploit this data, enabling them to escalate privileges and move laterally within the network, maintaining persistence and evading detection.
- **Enhanced Protection for AD**: Certes DPRM applies policy-based crypto-segmentation to protect AD from sophisticated attacks. This includes preventing unauthorised access and manipulation of sensitive data within the NTDS.dit file.
- **Policies to Define Data Flow**: Policies can define how to protect specific data flows and determine legitimate access points. Suspicious access outside approved directions can be flagged, helping to prevent unauthorised changes to privilege levels.

- **Mitigation of Lateral Movement and Privilege Escalation:** DPRM's unique segmentation and encryption approach significantly hampers the ability of attackers to move laterally within a network or escalate privileges, crucial steps in the attack chain. By anonymising data flows, it becomes impossible to identify which flows are valuable.

The ongoing action and threat from the likes of ShinyHunters highlights the urgent need for advanced security solutions capable of addressing sophisticated cyber threats, especially for those in data-rich industries. The group's history of high-profile attacks and their methodical exploitation of vulnerabilities should be a wake-up call for all organisations. Certes DPRM provides a robust defence against credential theft, AD compromise, and data exfiltration, offering unparalleled protection for critical infrastructure. By adopting a data-centric security approach, organisations can move beyond traditional perimeter defences and focus on protecting their most valuable assets.

Cyber threats are on the rise across all sectors, but the financial services sector faces an especially heightened risk due to the sensitive nature and volume of the data it handles. The recent breaches by ShinyHunters have put a spotlight on the vulnerabilities within this sector and the critical need for enhanced security measures. Network security measures alone are failing to prevent these sophisticated attacks. This is where Certes' DPRM offers a revolutionary approach by focusing 100% on the data rather than the infrastructure.

By implementing Certes DPRM, you can ensure that your organisation is protected against the ever-evolving landscape of cyber threats, secure your data, and maintain the trust of your stakeholders. Protect your organisation and secure your future with Certes DPRM, ensuring you stay ahead of cyber threats before they escalate.

> **Affecting 30 million people in just one breach, It's clear we need to rethink our approach to data security, focusing on making stolen data useless to attackers, rather than just trying to keep them out.**
>
> *Simon Pamplin – CTO, Certes*

Contact Certes

300 Corporate Center Drive,
Suite 140 Pittsburgh, PA 15108

1 (888) 833-1142
sales@certes.ai