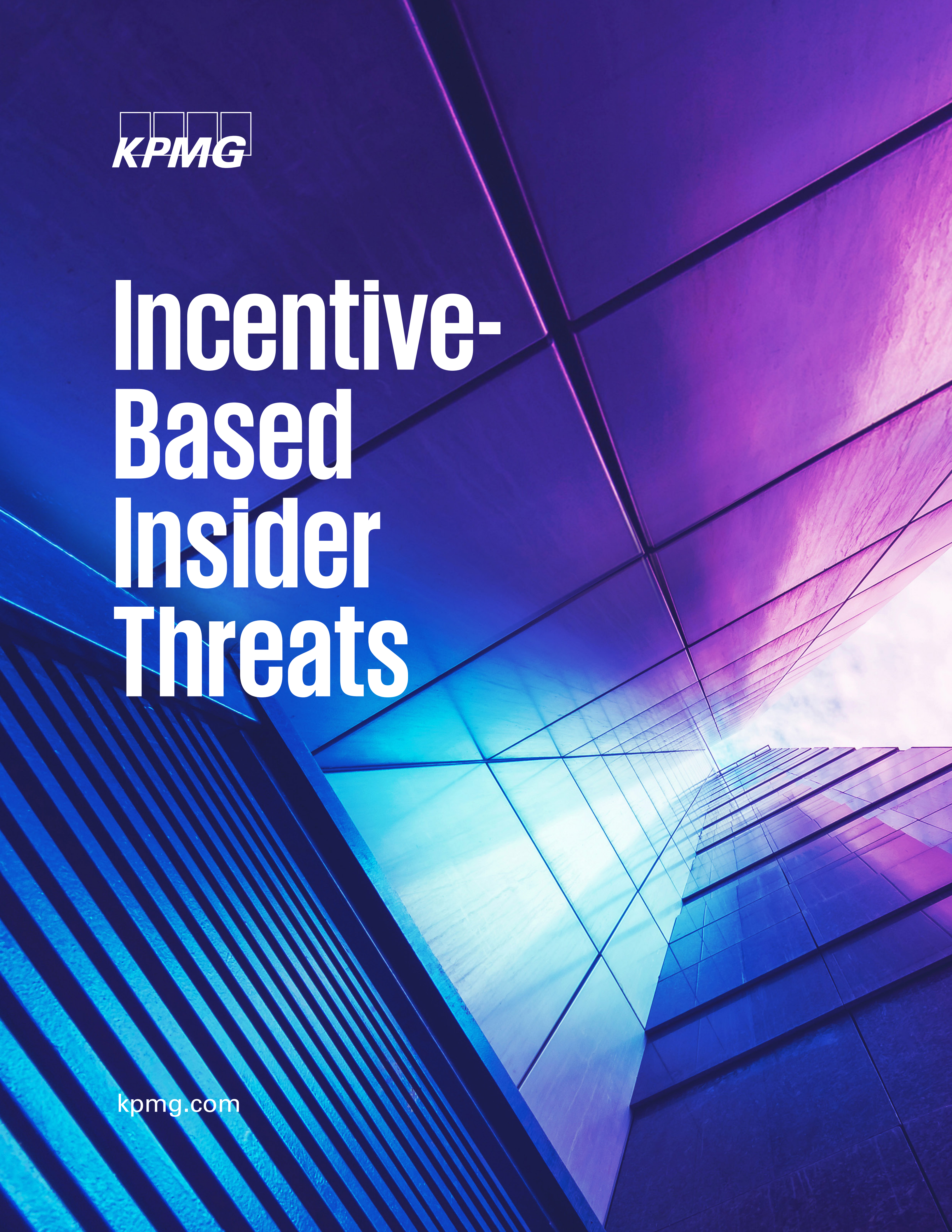

KPMG

Incentive-Based Insider Threats

kpmg.com

What does this mean and what can you do?

While the world is still deeply immersed in ratifying the new way of working two years since the onset of the COVID-19 pandemic as well as grasping the cyber ramifications of the Russian invasion of Ukraine, a third threat may be going unnoticed.

For organizations innovation is key to stay relevant and succeed in the marketplace and the same goes for the bad guys. Attackers are starting to shift from the typical attack vectors we are used to, and prepared for, and have since started offering incentives to insiders; payment in exchange for access. Attackers are starting to seek out individuals with legitimate access credentials at large organizations across industries to sell their VPN/VDI access. These individuals and groups are not looking for data so it can be believed that they are looking for insider credentials to gain an initial foothold into their targets to exfiltrate data and deploy ransomware payloads.

This emerging mindset of offering incentives to individuals in exchange for their access is an indication that the threats are changing. Attackers are supplementing the traditional tactics of extortion and trickery (i.e. phishing and social engineering) with bribery enabled by social media and the dark web; something that is much harder to protect against.

Ransomware groups have been successfully targeting large organizations for years with the goal of encrypting an organization's data to collect payment in exchange for decryption keys. While this tactic is by no means new, ransomware groups have been expanding into the data theft space to increase profits. This "double extortion" has proved effective in gaining additional revenue per attack and coercing victims to pay the ransom. However, the brazen public attempt to recruit insiders to sell their access is concerning especially considering current workforce sentiment among the "great resignation" and increasing competition for top talent.

What does this mean for targeted industries? Is this cause for concern or are adequate controls in place to make this a nonissue? Over the past decade, organizations have focused most of their efforts on forming a hardened shell around their networks to mitigate external attacks; but how do these protections stand up when the attacker has the keys to enter the kingdom?

Controls meant to mitigate the damage of credential theft become useless should the attacker be purchasing credentials from their rightful owner. Multifactor authentication has become the go-to control to further validate users and protect against compromised credentials through either a one-time passcode pushed to email/SMS or RSA tokens. However, this control only works if a credential is compromised, not if the owner of the account is compromised. It is safe to assume that the insider selling their credentials would include the method of MFA in the sale of their credentials, essentially making this control ineffective.

Device registration is another great control that can limit access to whitelisted devices; however, we face the same issue as MFA. The insider is most likely selling the registered device in addition to their credentials, making this control ineffective as well.

Additionally, leveraging a containerized environment through VDI is a great way to mitigate data loss, but the protections VDIs offer won't be effective if attackers have legitimate access to the environment.

While it may seem that all is lost, organizations have been heavily investing in insider threat preventative and detective controls to manage this risk. The following eight considerations can be a great starting place to help minimize the potential damage associated with sold accounts.

Protecting against a malicious insider threat is arguably one of the hardest things to do. While it may be impossible to prevent a user from selling their valid credentials to a bad actor, you can at least look to deter and detect unauthorized activity.

Geolocation may provide interesting context. Geolocation as an analytic input can provide mixed results, but seeing as TOR is not that evolved, it could maintain importance to UEBA, which may already have moved up the priority list given the fission and the current events with the Russia-Ukraine war. Detecting access from known bad IP addresses or suspicious locations can be a powerful indicator of a compromised credential that needs to be investigated and locked down.

Detect anomalies against a strong baseline. Understanding common user behavior requires a strong baseline of at least 90 days to minimize false positives. Understanding suspicious activity as it relates to the user profile can be a powerful way to detect a compromised account. This includes reviewing access times outside the norm, mass downloads from SharePoint, Confluence or other internal file shares, unusual access requests, etc. Use of UEBA and other risk scoring solutions can provide quick visibility into users who are exhibiting activities that could indicate credential compromise that can be further investigated.

Zero trust for zero chance. By always assuming actions are taken by an untrustworthy source, we can take better precautions that may isolate and identify a bad actor on the network. A zero trust strategy would provide a meaningful amount of risk mitigation, but takes time to orchestrate and operationalize with intentionality.

Cap data exfiltration. Data theft is of grave concern, especially when we consider recent incidents. In addition to ransomware, intellectual property and user/customer data are valuable targets for attackers. Having the capabilities to detect and prevent data uploads after a certain size becomes a valuable component in minimizing damage. Implementing data caps on uploads that can either be static, or the same across the organization, or dynamic, based on strong baselines, can help minimize the amount of data that can be exfiltrated. And to combat the attackers that take the slow and steady approach to data theft, implementing a time-bound data cap, i.e., blocking all uploads after xGb within the past 7 days unless provided an exception, can be effective.

Network segmentation + strong IAM controls = isolation. Coupling a sound network segmentation strategy with strong IAM controls, as it relates to entitlement management across user and privileged accounts, might not be able to prevent a malicious actor purchasing and using credentials, but it can isolate and limit what can be done with the purchased credentials.

Perfect PAM Practices. Use of a PAM solution can help with mitigation, alongside vault usage for addressing passwordless SSH keys, API keys, PEM files, and other access methods. Additionally, local admin account password management is another vector and having good attack surface management to see if these credentials are being used on public facing infrastructure can help detect credential misuse.

Force onsite execution of critical activities. There could be significant advantage to having a physical connection to offices for sensitive transactions. Similar to how banks require onsite access for transaction efficiency, but for cyber.

If you can't prevent, deter. Without sounding like a police state, reinforce user awareness that your organization has sophisticated monitoring controls in place and that malicious activity is taken seriously and treated as a grave offense. Remind users that malicious attacks on the company will not be tolerated and may result in the involvement of law enforcement. If you can't prevent the sale of credentials, the existence of harsh penalties may deter the sale.

Authors:

Matt Miller
Principal
Cyber Security Services
InsiderThreat Co-Lead
E: matthewpmiller@kpmg.com

Brad Raiford
Director
Cyber Security Services
E: braiford@kpmg.com

Joe Mazzella
Manager
Cyber Security Services
InsiderThreat Co-Lead
E: jmazzella@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.