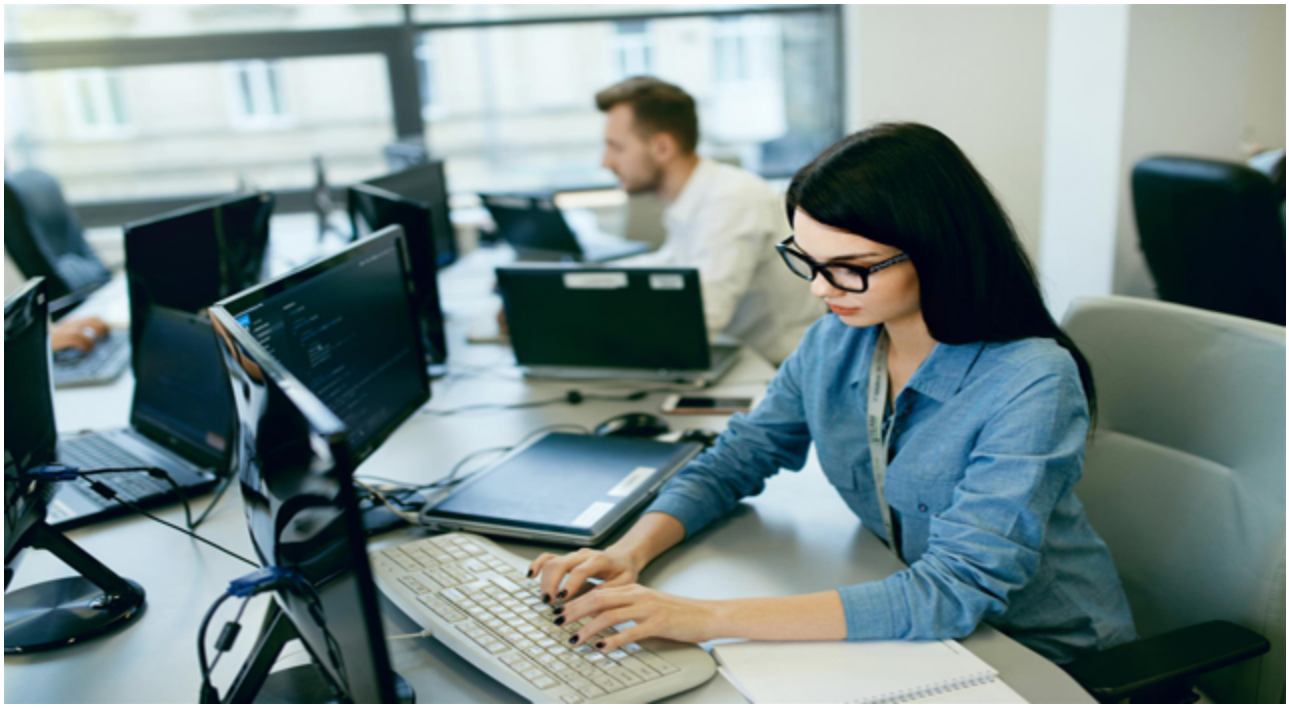
Research, News, and Perspectives

blog.trendmicro.com/trendlabs-security-intelligence/account-with-admin-privileges-abused-to-install-bitpaymer-ransomware-via-psexec



Exploits & Vulnerabilities

Celebrating 15 Years of Pwn2Own

Join Erin Sindelar, Mike Gibson, Brian Gorenc, and Dustin Childs as they discuss Pwn2Own's 15th anniversary, what we've learned, and how the program will continue to serve the cybersecurity community in the future.

Latest News May 25, 2022

Save to Folio

Latest News May 25, 2022

Save to Folio

Content added to Folio

Compliance & Risks

S4x22: ICS Security Creates the Future

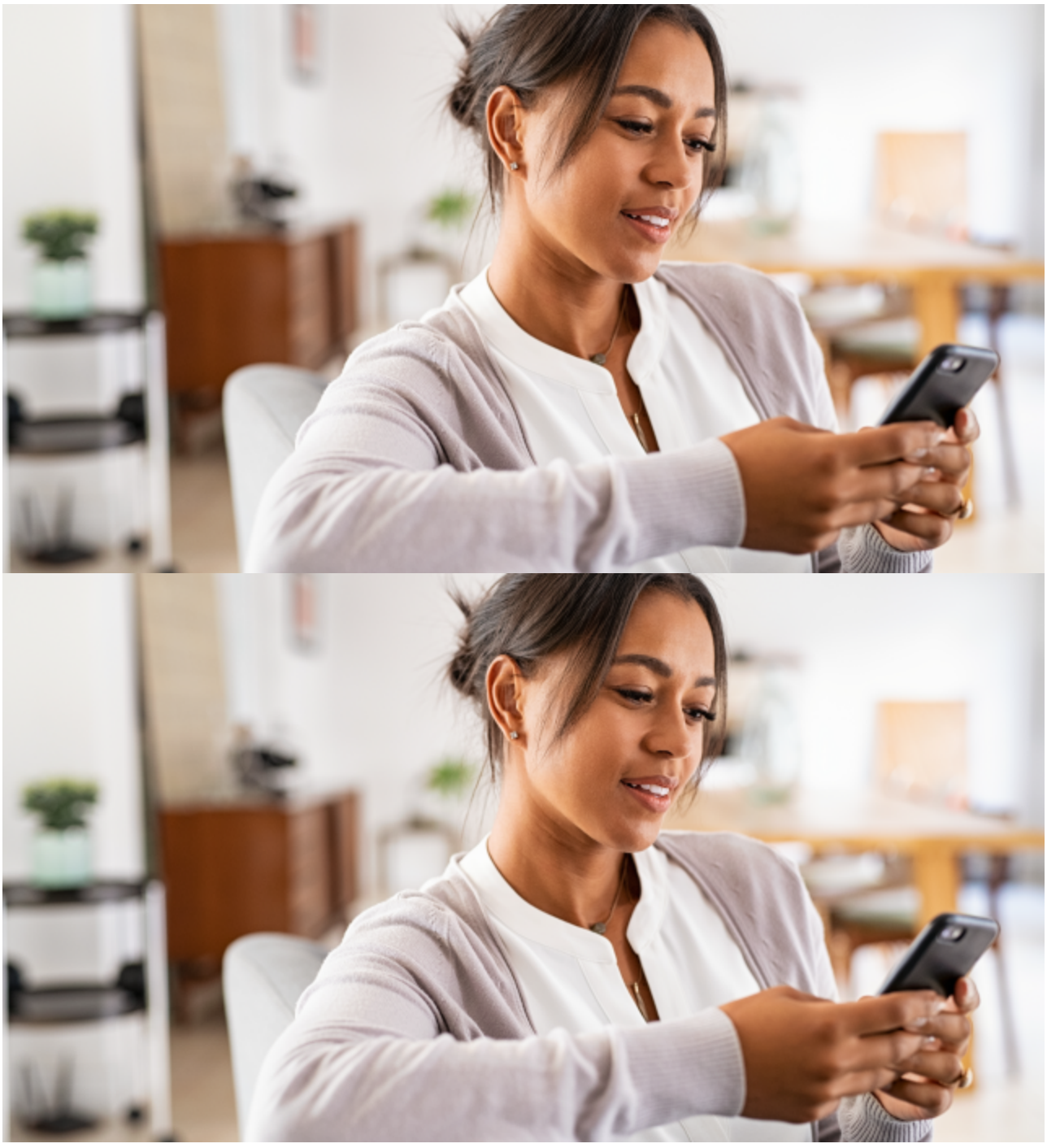
The ICS Security Event S4 was held for the first time in two years, bringing together more than 800 business leaders and specialists from around the world to Miami Beach on 19-21 Feb 2022. The theme was CREATE THE FUTURE.

Security Strategies May 12, 2022

Save to Folio

Security Strategies May 12, 2022

Save to Folio



Compliance & Risks

Security Above and Beyond CNAPPs

How Trend Micro’s unified cybersecurity platform is transforming cloud security

Security Strategies May 10, 2022

Save to Folio

Security Strategies May 10, 2022

Save to Folio

Bruised but Not Broken: The Resurgence of the Emotet Botnet Malware

During the first quarter of 2022, we discovered a significant number of infections using multiple new Emotet variants that employed both old and new techniques to trick their intended victims into accessing malicious links and enabling macro content.

Research May 19, 2022

Save to Folio

Research May 19, 2022

Save to Folio

New APT Group Earth Berberoka Targets Gambling Websites With Old and New Malware

We recently found a new advanced persistent threat (APT) group that we have dubbed Earth Berberoka (aka GamblingPuppet). This APT group targets gambling websites on Windows, macOS, and Linux platforms using old and new malware families.

April 27, 2022

Trend Micro's One Vision, One Platform

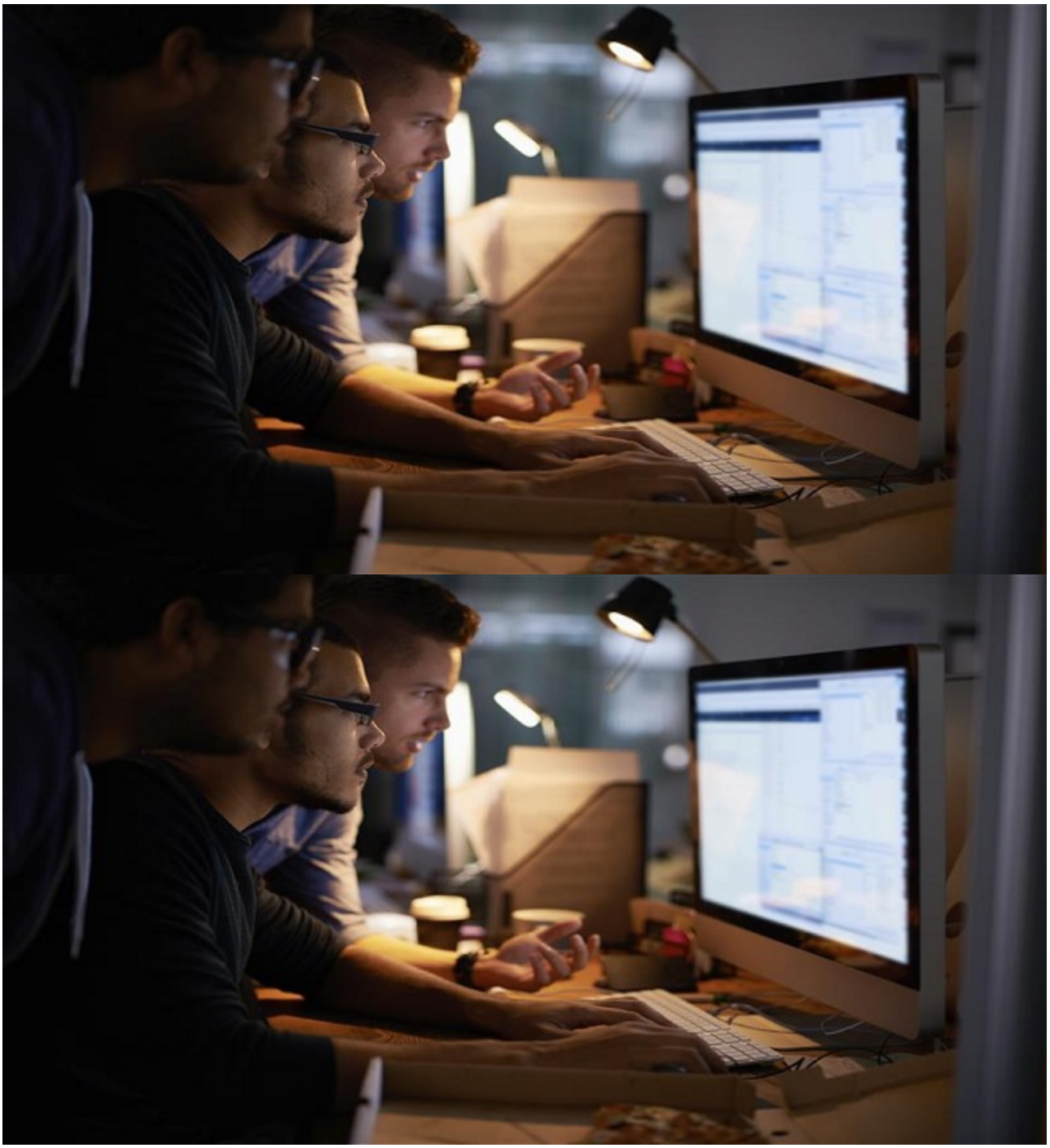
Why Trend Micro is evolving its approach to enterprise protection

Security Strategies May 17, 2022

Save to Folio

Security Strategies May 17, 2022

Save to Folio



Ransomware

New Linux-Based Ransomware Cheerscrypt Targets ESXi Devices

Trend Micro Research detected “Cheerscrypt”, a new Linux-based ransomware variant that compromises ESXi servers. We discuss our initial findings in this report.

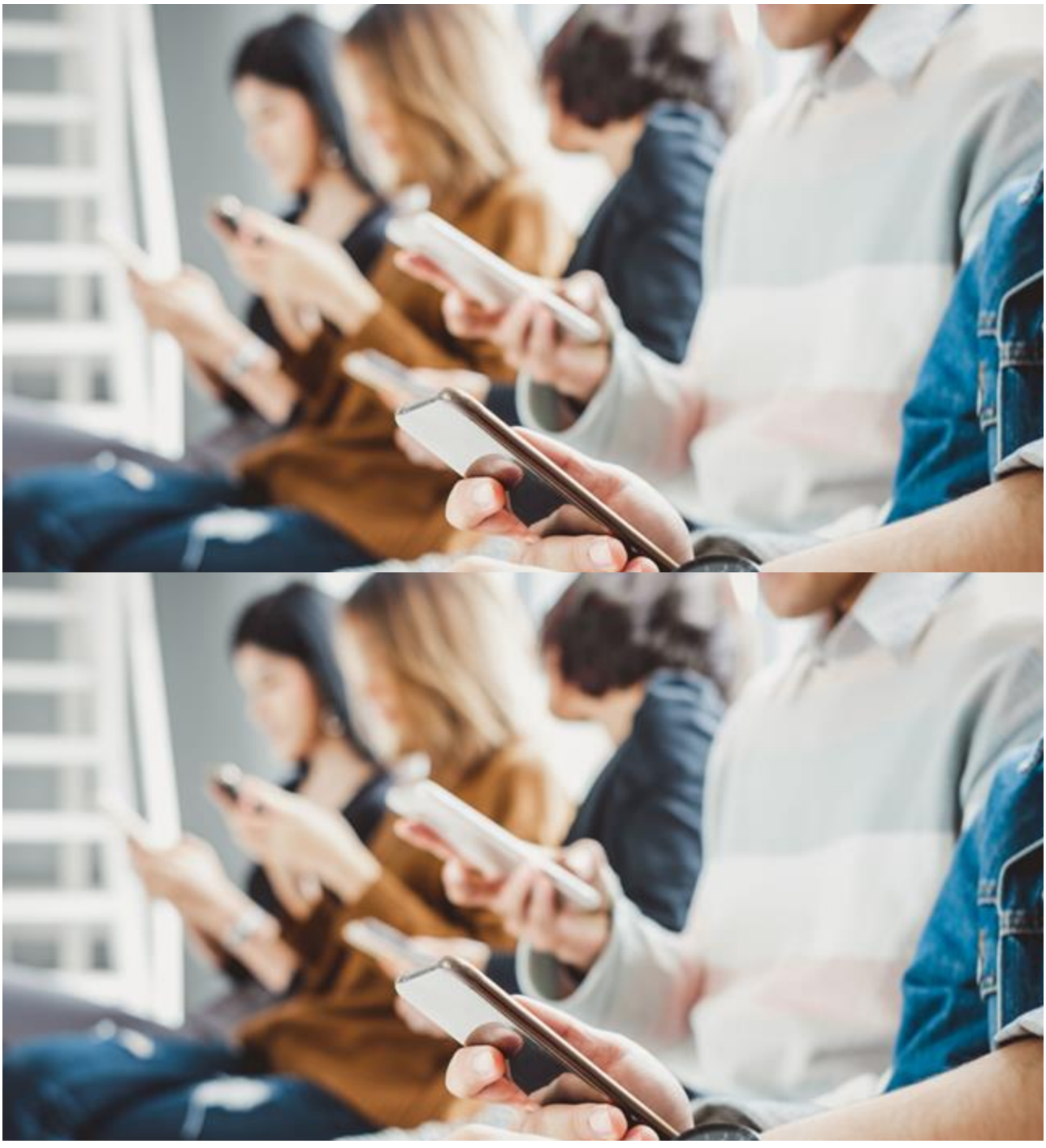
Research May 25, 2022

Save to Folio

Research May 25, 2022

Save to Folio

Subscribe



Mobile

Fake Mobile Apps Steal Facebook Credentials, Cryptocurrency-Related Keys

We recently observed a number of apps on Google Play designed to perform malicious activities such as stealing user credentials and other sensitive user information, including private keys.

Research May 16, 2022

Save to Folio

Research May 16, 2022

Save to Folio

Uncovering a Kingminer Botnet Attack Using Trend Micro™ Managed XDR

Trend Micro’s Managed XDR team addressed a Kingminer botnet attack conducted through an SQL exploit. We discuss our findings and analysis in this report.

Research May 18, 2022

Save to Folio

Research May 18, 2022

Save to Folio

Cloud

The Fault in Our kubelets: Analyzing the Security of Publicly Exposed Kubernetes Clusters

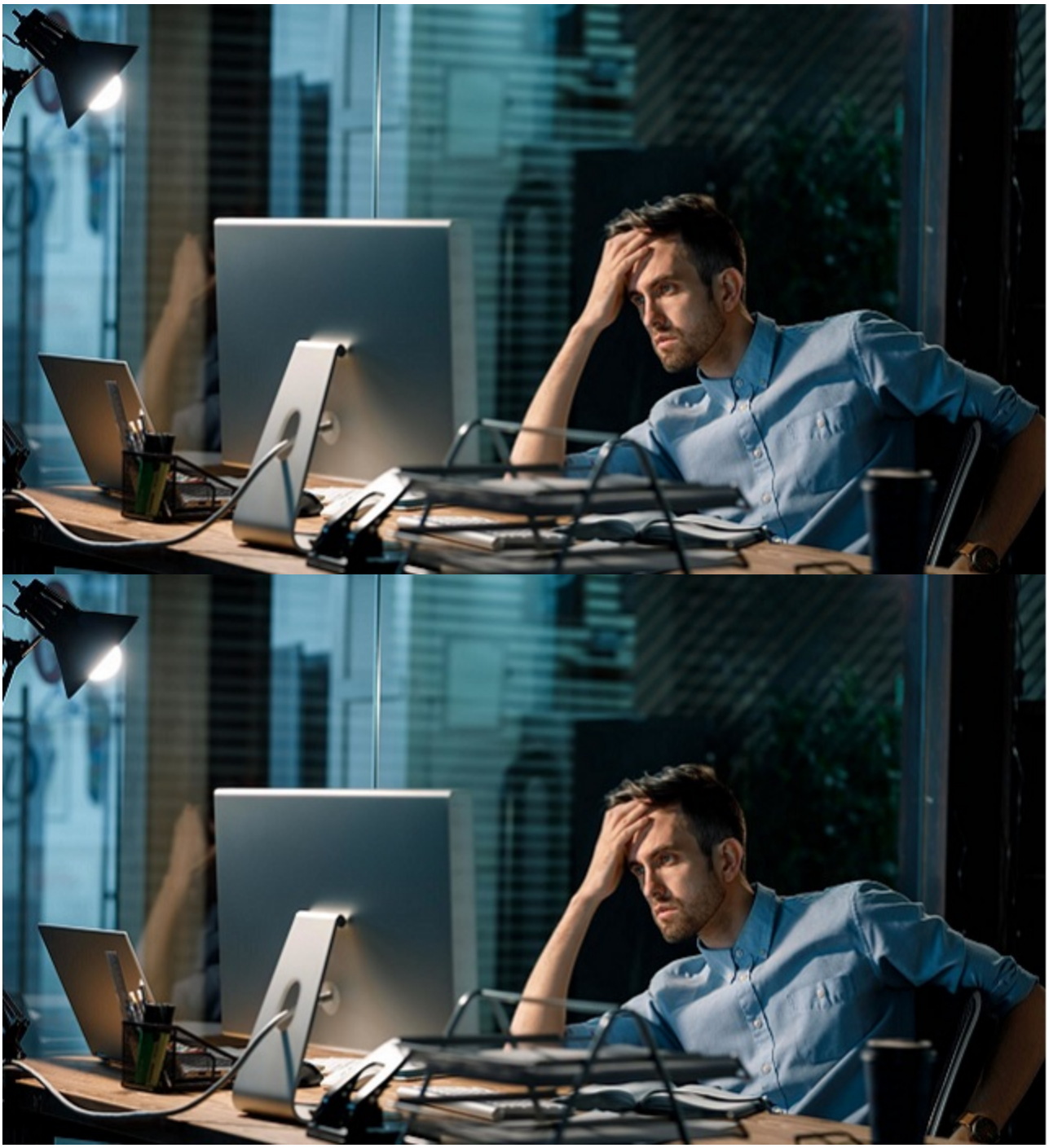
While researching cloud-native tools, our Shodan scan revealed over 200,000 publicly exposed Kubernetes clusters and kubelet ports that can be abused by criminals.

May 24, 2022

Save to Folio

May 24, 2022

Save to Folio



Ransomware

Examining the Black Basta Ransomware's Infection Routine

We analyze the Black Basta ransomware and examine the malicious actor's familiar infection tactics.

Research May 09, 2022

Save to Folio

Research May 09, 2022

Save to Folio