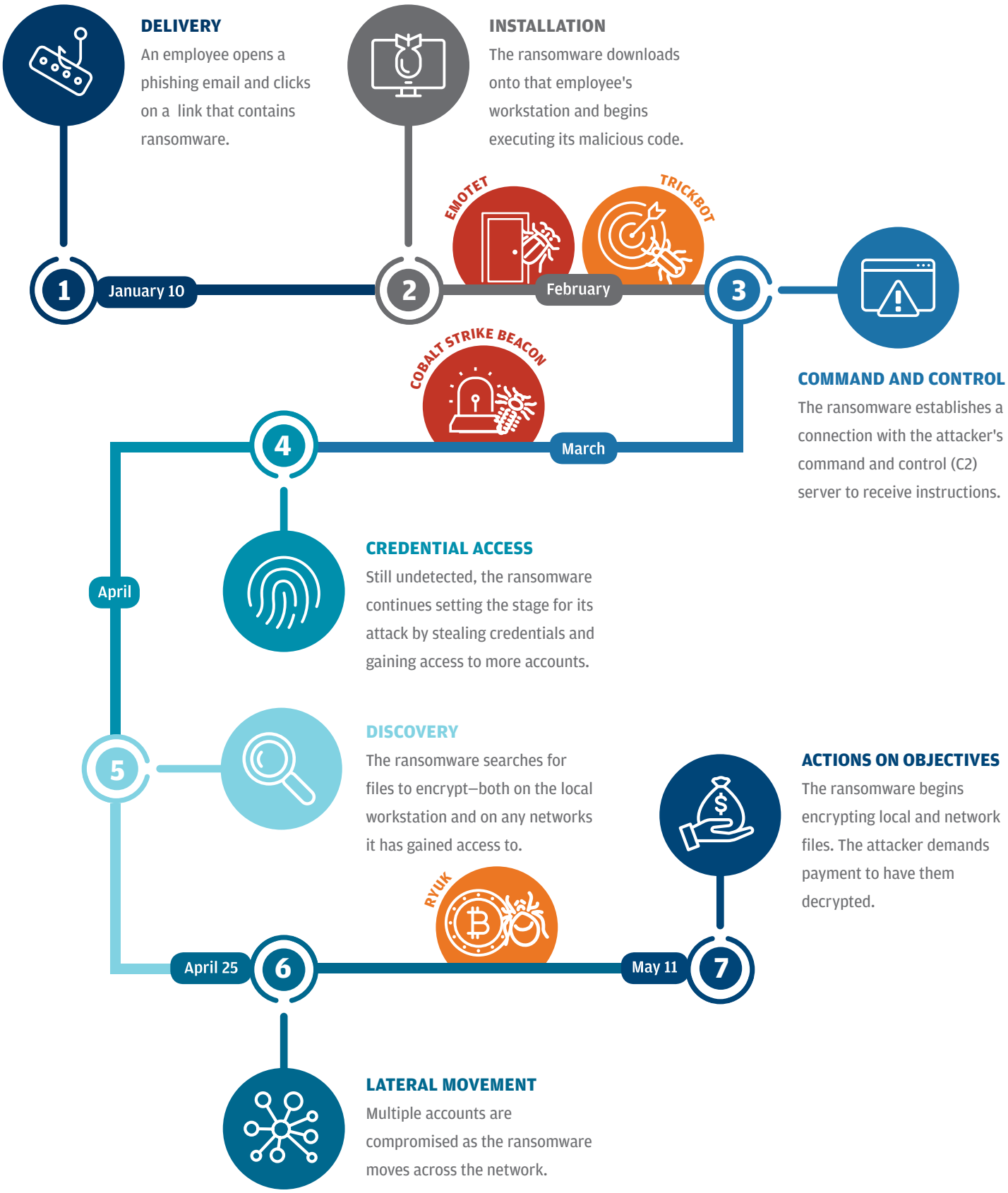
THE ANATOMY OF A RANSOMWARE ATTACK

Ransomware attacks are growing more sophisticated. Learn how they unfold and how you can prepare for the worst-case scenario.

Most businesses are probably familiar with ransomware—a type of malware that criminals use to extort organizations by encrypting and holding their data hostage until they make a digital payment.

What many may not know is that ransomware can lie undetected in an exposed organization's systems for days, weeks or even months before it's revealed through a ransom demand. Use the graphic below to follow the trail of a ransomware attack involving multiple malware strains that infiltrated an organization over the course of five months—ultimately impacting more than 11,000 servers and workstations.

The 7 Stages of Ransomware Attacks



Key: Malware Strains

EMOTET
Steals information, executes backdoor commands and delivers Ryuk payload.

TRICKBOT
Often paired with Emotet—steals login credentials and identifies targets for Ryuk ransomware.

COBALT STRIKE BEACON
Using a custom implant called "Beacon" this malware helps facilitate C2 and lateral movement.

RYUK
The final malware dropped in the attack—this ransomware encrypts systems, devices and files until a Bitcoin ransom is paid.

MAZE
A new, sophisticated form of ransomware that steals private data in addition to encrypting local and network files. Criminals then threaten to release the stolen data if the ransom is not paid.

How to Ensure Your Organization Is Resilient

The best protection against ransomware is to prepare for the worst-case scenario: major disruption across the full scope of your IT infrastructure. Some steps you can take to help plan for and respond to a ransomware attack include:

- Perform a Business Impact Analysis (BIA) to predict the consequences of ransomware disruption and gather information to develop recovery strategies.
- Create multiple backups to restore critical systems if the criminals delete your files (this sometimes occurs even after the ransom is paid). Ensure one set of backups is offline and inaccessible from your organization's network.
- Contact your financial institution if you are impacted by ransomware or any malware so they can be on high alert for any anomalous activity.
- >> Contact law enforcement including the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3).
- >> Provide training and education for employees on how to identify and respond to suspicious emails and conduct phishing exercises.
- Contact your financial institution before attempting to pay a ransom to determine whether the financial institution can facilitate the ransom payment.
- Consider purchasing a cyber insurance policy—designed to mitigate risk exposure—that covers ransomware.