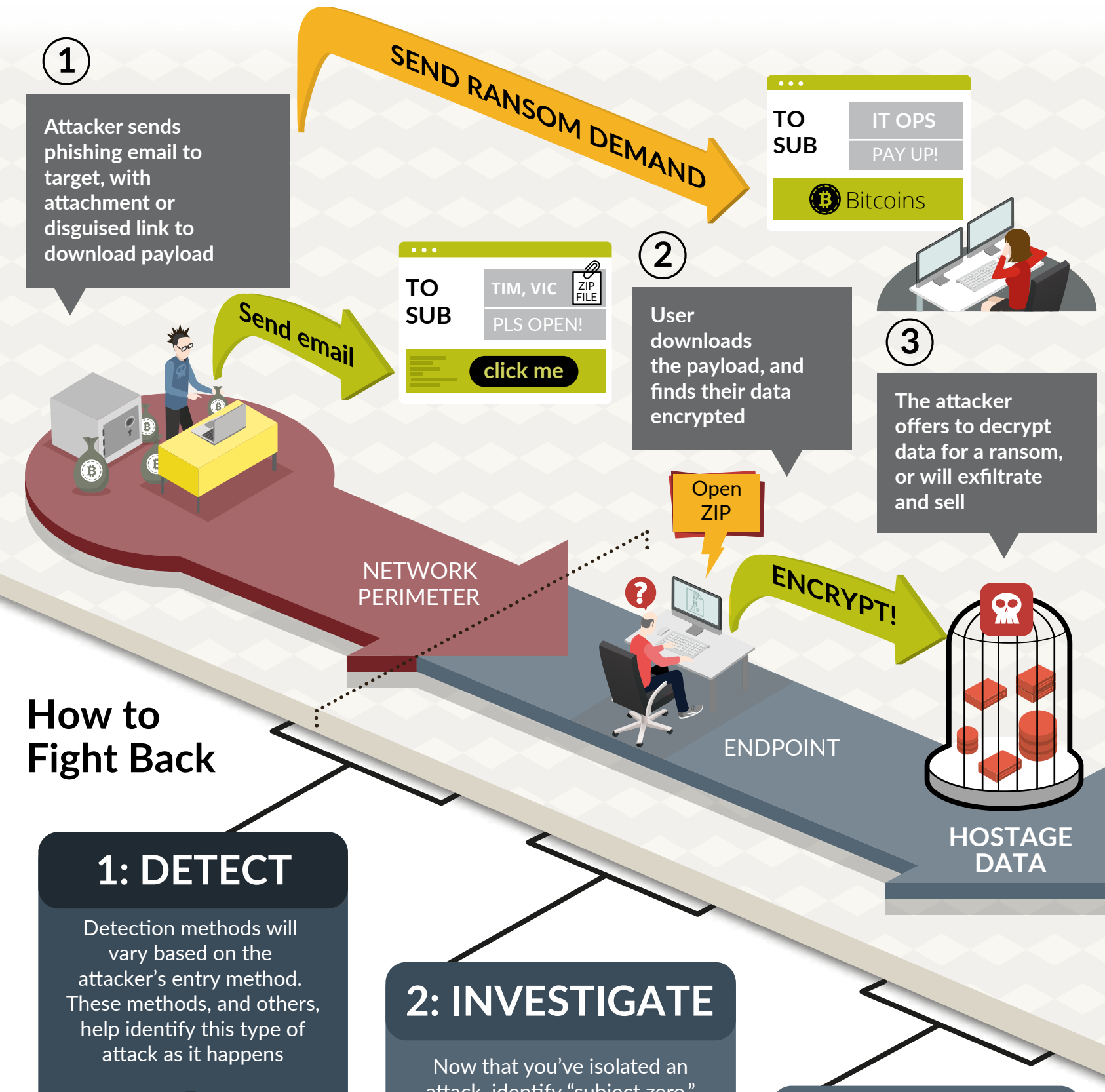
NETWITNESS

Detecting and Responding to a Ransomware Attack

Ransomware attackers are motivated entirely by money, and they go after your high-value data. If they gain control of it, through encryption or other means (93% of phishing attacks arrive by email[1]), they can force you to pay to get it back. That is, unless you have the ability to detect these attacks and stop them in their tracks. Here's how one common type of Ransomware exploit happens, and what can be done to stop it.



How to Fight Back

1: DETECT

Detection methods will vary based on the attacker's entry method. These methods, and others, help identify this type of attack as it happens

Track URL GET with unusually large download

Track emails with mismatch between link text and URL

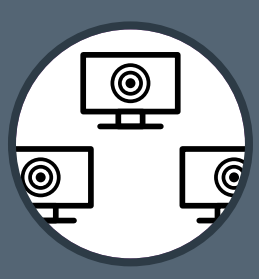
Report downloads of zip, dll, vbs, etc. files from emails

Report large outbound encrypted sessions

2: INVESTIGATE

Now that you've isolated an attack, identify "subject zero," then look deeper and broader throughout your network for other events that might be related

Automatically extract key evidence through consistently updated threat intelligence. Reconstruct attack and analyze payload.



Look laterally at systems the infected machine communicates with

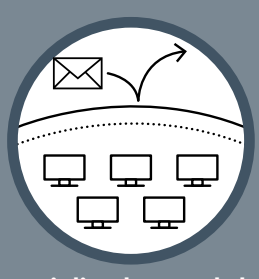
Search your network for other endpoints that have been targeted by the same attack

Pinpoint precise time of attack and last known good state

3: RESPOND

Employ your recovery processes and technologies to contain the impact and recover as quickly as possible

Use automatic playbooks to quarantine malicious activity, contain the attack and limit its' impact



Memorialize learned threat behavior and block future attacks

Restore data from backup to minimize loss

Congratulations! You've removed the attacker's hold on your data, and don't need to pay a ransom!

Learn more at **netwitness.com**

1. Verizon 2021 Data Breach Investigation Report, https://www.verizon.com/business/en-gb/resources/reports/dbir/