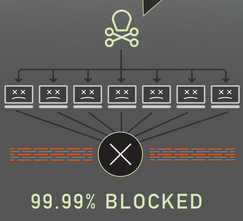
# The DDoS ransom.

HOW A TARGETED DDOS ATTACK WAS FORCEFULLY DEFEATED IN 3 HOURS

YOUR MONEY OR YOUR DATA

1 Armor DDoS mitigation controls block 99.99 percent of all malicious traffic. But these sophisticated threat actors thought their DDoS attack could circumvent battle-tested perimeter defenses. They were wrong.

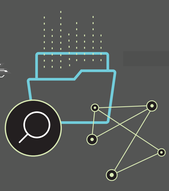


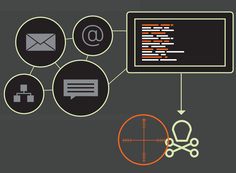
99.99% BLOCKED

50 ฿ FOR YOUR NETWORK

2 Shortly after the start of the DDoS attack, the customer received a ransom notice demanding 50 Bitcoins to end the assault. But Armor was already on the case.

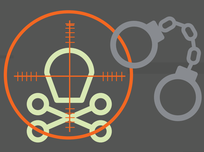
3 Armor's Threat Resistance Unit, or TRU, examines the attack, collecting packet and traffic information. From this data, they build a TTP — Tactics, Techniques and Procedures — for attack attribution.

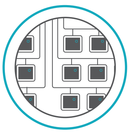


4 Based on gathered intelligence, Armor confirms it was a targeted DDoS attack by a known group of mid-skill-level threat actors.

5 Armor notifies the FBI, Secret Service and Royal Canadian Mounted Police to take action. Arrests pending.



## INTERNAL AFTER-ACTION REPORT SUMMARIZES THE ATTACK EVENT



CUSTOMER ENVIRONMENT NEVER IMPACTED OR COMPROMISED, COSTLY FORENSICS AVOIDED

THREAT ACTORS IDENTIFIED & NO RANSOMS PAID

ARMOR'S ELITE OPERATIVES PROVED EFFECTIVE

—

TOTAL RESOLUTION TIME: 3 HOURS

# Your data doesn't belong to them.

## WE WON'T LET THEM TAKE IT.

ARMOR™

THE FIRST TOTALLY SECURE CLOUD COMPANY™