CISO GLOBAL

TALKING TACTICS:

Cybersecurity Defensive Tactics for Common Attack Types

COMPROMISED ACCOUNT

?	🚨	🔍	👆
Attacker gains access to internal account	Off-hour logins Group changes Abnormally high network traffic	Active directory logs OS logs Network traffic Contact user	Disable the account Change the password Forensic investigation

BRUTE FORCE

?	🚨	🔍	👆
Attacker attempting access through multiple passwords	Multiple login failures in a short period of time	Active directory logs Application logs System logs Contact user	Disable the account Block and investigate the attacker

SYMBOL KEY

?	🚨	🔍	👆
What is it?	Indicators	Investigation Locations	Possible Actions

3 BOTNETS

Software runs automated tasks on victims' devices, usually to create DDOS attacks

Connections to suspicious IPs

Abnormally high volume of network traffic

Network traffic

OS logs

Contact server owner

Contact support team

Isolate server

Remove malicious processes

Patch the vulnerability

4 RANSOMWARE

Malware encrypts selective files on a device and creates a ransom note

Anti-virus alerts

Connections to suspicious IPs

High volume of file changes/update logs

AV logs

OS logs

Account logs

Network traffic

Isolate the device

Run anti-virus from USB or external drive (not compromised AV)

DATA EXFILTRATION

?

Sensitive data being copied/moved out of the environment without authorization

Abnormally high network traffic

Connections to cloud storage solutions (Box, Dropbox, AnonFTP, etc.)

Unusual USB stick

Network traffic logs

Proxy logs

OS logs

Isolate the device

Disconnect from network

Run full forensic analysis

DENIAL OF SERVICE (DDOS)

?

Intentional paralysis of a network by flooding it with data from several devices

Abnormally high network traffic towards a specific device

Network traffic logs

Firewall logs

OS logs

Contact ISP

Apply needed patches

Contact network support

ADVANCED PERSISTENT THREATS (APTS)

State sponsored attackers that compromise networks and create back doors

Connection to suspicious IPs

Abnormally high network traffic

Off-hours access logs

New Admin accounts

Network traffic logs

Access logs

OS logs

Contact server owner

Isolate the device

Run full forensic analysis (hard to detect)

If you need help with Cyber Incident Response, we're here for you.

Responding to a security incident requires experts who know how to identify and mitigate an immediate threat, investigate underlying vulnerabilities that led to the threat, address any regulatory compliance implications, and restore order right away. With its own, fully-staffed, 24x7x365 Security Operations Center, CISO Global has the highly trained security analysts, advanced tool sets, security clearance levels, and years of expertise to provide a fully coordinated Incident Response team to restore order during what can feel like a chaotic event for any organization.

LEARN MORE

CISO
GLOBAL