



Creative ITC



ARCTIC  
WOLF

# EVERY MINUTE MATTERS

EVERY 11 SECONDS A BUSINESS FALLS  
VICTIM TO A RANSOMWARE ATTACK

**BUT IT TAKES FIRMS...**

## 261 DAYS

ON AVERAGE TO **IDENTIFY AN ATTACK**

## 314 DAYS

ON AVERAGE TO **CONTAIN A BREACH**

Organisations need to quickly detect and  
remediate cyber-attacks to stay protected.

CREATIVE ITC'S SECURITY OPERATIONS CENTRE AS A SERVICE (SOCaaS)  
SOLUTION PROVIDES CLIENTS WITH AN **IMMEDIATE RESPONSE TO THREATS 24/7**  
AND APPLIES THIS LEARNING TO STRENGTHEN RESILIENCE OVER TIME.

## RANSOMWARE RESPONSE TIMELINE

THIS TIMELINE OUTLINES RAPID RESPONSE  
TO A REAL-WORLD RANSOMWARE ATTACK

■ Arctic Wolf Platform ■ Triage Team ■ Customer ■ Concierge Security Team

**5:23 AM**

### SOURCE: ACTIVE DIRECTORY

- [USER1] user account begins logging into multiple systems



**5:26 AM**

### SOURCE: ARCTIC WOLF SENSOR

- HTTP header information containing outbound communication with xx.xxx.230.236 detected, possible C2
- Suspected PowerShell Empire activity detected on [SERVER1]



**5:28 AM**

### INVESTIGATION TRIGGERED

- C2 traffic is correlated with PowerShell Empire activity on [SERVER1]
- The incident is escalated to Triage Team Level 3 forensics dashboard with Urgent status



**5:29 AM**

### INVESTIGATION STARTS

- Triage team begins investigation and finds activity within Active Directory logs of [USER1] user logging into many systems in a short amount of time
- Confirms network and PS Empire alerts are a true positive and assess scope of attack



**5:48 AM**

### INCIDENT TICKETED

Investigation concludes and Triage Team contacts customer with a CSV detailing the C2 traffic as well as logins which preceded these connections. Gives recommendation to:

- Contain the device / disconnect from network
- Change passwords for the [USER1] accounts / Service accounts from network
- Run AV scan on endpoints



**6:13 AM**

### REMEDIATION

- Customer responds that the device has been contained and passwords reset

### SECURITY JOURNEY

CST works with customer to identify areas of improvement for their security posture:

- Implement principle of at least privilege for remote tools
- Geofence firewalls
- Enable MFA
- Setup GPO to block use of PowerShell
- Install Arctic Wolf Agent with Sysmon on all machines



## 5 MINS

TO **DETECT** THE ATTACK

## <1 HOUR

TO **CONTAIN** THE BREACH



Creative ITC



ARCTIC  
WOLF

Interested in hearing more about how our 24/7 fully  
managed SOCaaS solution could ensure your organisation  
benefits from a more robust, proactive security posture?

[hello@creative-itc.com](mailto:hello@creative-itc.com) | +44 (0)20 4551 9267