UnderDefense
CYBERSECURITY

# Black Basta Ransomware Stopped in ⏱ 43 Minutes: Inside a Real Managed Detection & Response Case

Our customer is a top-tier Swiss outdoor equipment brand with 1,000+ employees and a global footprint. With over $250M in annual revenue, ensuring operational resilience and customer trust is key to staying competitive.

**43 MIN**
Ransomware attack stopped

**100%**
Staff trained

**40%**
Faster response time

**$4.5–20M**
Losses prevented

## CLIENT INTRODUCTION

| | | | |
|---|---|---|---|
| **Headquarters:** | Switzerland | **Employees:** | 1,000+ |
| **Industry:** | Outdoor equipment | **Annual Revenue:** | over $250M |
| **Technologies:** | Microsoft Defender | **Project Duration:** | November 2024 and ongoing |

## Background

In December 2024, the UnderDefense Managed Detection and Response (MDR) team began documenting a series of sophisticated social engineering attacks orchestrated by **Black Basta ransomware operators**. These attacks primarily targeted customer support employees, who are often less familiar with cybersecurity protocols.

The infection chain typically began with a spam email campaign that inundated employees with over **3,000 unrelated emails**, making it difficult for them to discern legitimate communications from malicious ones. Following this barrage, attackers would impersonate IT support personnel, leveraging social engineering tactics to gain remote access to victims' workstations through tools like **Quick Assist**. Once inside, they would install **DarkGate C2 malware**, setting the stage for further exploitation and potential ransomware deployment.

## Challenges

- ? Sophisticated social engineering - Attackers impersonated IT support to deceive employees.
- ? High-volume phishing - Up to 50 spam emails per minute caused confusion
- ? Delayed reporting - Employees submitted IT tickets instead of alerting Security.
- ? IT impersonation - Employees trusted fake internal communications
- ? Lack of clear escalation paths - Employees were unsure how to report threats.

## Results

- ✓ Faster Response - Reduced TTA to 5 minutes and TTR to 43 minutes.
- ✓ 40% Faster Threat Remediation - Quicker containment and resolution.
- ✓ Improved Incident Reporting - Faster escalation and response
- ✓ 100% Cybersecurity Awareness Training Stronger defense against phishing.
- ✓ Reduced Unauthorized Access Risk - Blocked untrusted domains and restricted remote access.

# The Solution

To address these challenges, UnderDefense implemented a multi-faceted approach:

1 **Communication Protocols:** A reliable communication channel was established between the Security team and other departments, allowing employees to report potential breaches directly and without delay. This included creating a dedicated hotline and email address for security concerns, ensuring that employees could quickly escalate issues without navigating the slower IT support ticketing system.

2 **Security Awareness Training:** The corporate security awareness program was revamped to include training on modern social engineering tactics, such as email bombing and impersonation scams. Employees were educated to recognize suspicious communications and the importance of verifying the identity of anyone requesting sensitive information or access to their devices. Regular drills and simulated phishing attacks were introduced to reinforce these lessons.

3 **Technical Mitigations:**

- **Email Filtering:** Untrusted top-level domains were blocked via Microsoft Exchange to reduce the volume of spam emails reaching employees. For instance, domains associated with known threat actors, such as those ending in ".ru" and ".ir," were restricted.
- **Remote Access Controls:** The use of remote access tools like Quick Assist was restricted through Intune and AppLocker, ensuring that only authorized personnel could utilize these tools for legitimate purposes.
- **Enhanced EDR Management:** The existing Endpoint Detection and Response (EDR) solution was fine-tuned to require experienced operators for effective monitoring and remediation. This included configuring the EDR to operate in prevention mode and blocking known malicious files and behaviors before they could execute.

# Complete Timeline

A seemingly harmless email flood quickly escalated into a full-scale cyber attack—from phishing to lateral movement and, ultimately, a high-risk CobaltStrike deployment. This timeline breaks down the key attack stages, how the adversaries exploited human and technical weaknesses, and the mitigation strategies we used to stop the threat before it turned into a full-blown ransomware incident.

1 **Targeted email spam attack (December 2024):** A group of non-technical employees from the customer support department received over 3,000 unrelated emails, with a rate of up to 50 emails per minute. The attackers subscribed the victims to various services and marketing lists to bypass email protection solutions. The emails were difficult to correlate and block, leading to panic among employees who feared their accounts had been breached.

2 **Teams call to Quick Assist (shortly after the email attack):** All targeted customer support employees received Microsoft Teams calls from attackers impersonating the company's IT support. One victim approved a Quick Assist connection, allowing the attackers to download a malicious ZIP archive containing the DarkGate C2 agent disguised as “SystemSync.exe.” The attackers misled the victim into believing they were resolving the email spam issue.

### Mitigation strategies we used:

- **Restrict MS Teams communications:** Block all Microsoft Teams calls and messages originating from or directed to external and untrusted users. For more information, refer to the Microsoft Teams External Access documentation.
- **Firewall configuration for Quick Assist:** Implement firewall rules to block Quick Assist DNS domains unless they are being utilized for corporate purposes. Detailed guidance can be found in the Quick Assist Client Management documentation.
- **Limit remote access tools:** Enforce restrictions on the use of remote access tools such as Quick Assist, TeamViewer, and AnyDesk through Intune and AppLocker, or by leveraging an existing EDR solution. For further details, see the AppLocker Configuration documentation.

3 **DarkGate C2 activity (following the Quick Assist session):** The **DarkGate C2 agent** performed system discovery and downloaded a second-stage payload via **PowerShell. T**his payload utilized **AutoIt3** for persistence and injected shellcode into a legitimate **Microsoft Edge** process to evade detection. The attackers gained remote access to the workstation and were able to move laterally within the **Active Directory domain.**

### Mitigation strategies we used:

1. **Deploy a robust antimalware solution:**
   Install a reliable Endpoint Detection and Response (EDR) solution on all corporate devices. For more information, refer to our blog post on EDR.
2. **Configure EDR for prevention:**
   Ensure that the antimalware solution is configured to operate in prevention (blocking) mode.
3. **Implement a corporate VPN or Zero Trust Network Access solution:**
   a. Route all user traffic through the selected VPN or Zero Trust Network Access (ZTNA) solution.
   b. Monitor and analyze the domains that users access to identify potential threats.
   c. Integrate the VPN or ZTNA solution with threat intelligence feeds to enhance security.
4. **Block Untrusted Domains:**
   a. Proactively block untrusted top-level domains (TLDs) such as ".shop" or ".monster" to reduce exposure to malicious sites.
   b. Additionally, block any domains identified in the connected threat intelligence feeds to further protect the network.

4 **From DarkGate to CobaltStrike (one day later):** The attackers used the existing **DarkGate C2** to deploy a **CobaltStrike** beacon, a more powerful tool for privilege escalation and credential access. The CobaltStrike beacon went undetected by the existing EDR solution, allowing the attackers to execute their plans without immediate intervention.

### Mitigation strategies we used:

Restrict executions from common staging folders: Implement measures to block the execution of files from frequently used staging directories, including:

- C:\
- C:\temp\
- C:\ProgramData\
- C:\Users\Public\
- C:\Windows\Temp\
- C:\Users*\AppData*

5 **CobaltStrike C2 activity (immediately after deployment):** Shortly after deployment, the threat actors began utilizing CobaltStrike to enumerate local users, gather information about the domain and domain controllers, and attempt to retrieve privileged domain identities for further exploitation. Initially, they employed the binary "**C:\temp\22x64.exe,**" which was configured to beacon via HTTPS. However, they later transitioned to using **"C:\temp\15DNSx64.exe,"** which was capable of DNS TXT beaconing. The reason for this switch remains unclear.

### Mitigation strategies we used:

The MDR team was alerted soon after the beaconing commenced and intervened to manually halt the attack, as the existing **EDR solution failed** to automatically remediate the threat. Without timely and effective remediation, this incident could have escalated into a double-extortion attack involving both ransomware encryption and data exfiltration, as evidenced by previous campaigns conducted by **Black Basta.**

## Outcomes

Quick action, smart security measures, and better employee awareness made all the difference. By tightening response times and improving how threats were reported, we didn't just stop the attack—we made sure it wouldn't happen again. Here's what changed:

### Faster Incident Response

- First response was in 5 minutes, with escalated cases handled in 14 minutes.
- Threats were fully contained in 43 minutes, cutting remediation time by 40%.

### Better Threat Reporting

- Employees stopped hesitating and started reporting threats faster thanks to clearer communication protocols.
- Security teams could react immediately instead of sorting through IT tickets.

### Stronger Cyber Awareness

- 100% of employees are trained to spot and stop phishing attempts before they cause damage.
- Staff became more confident in recognizing scams and working with security teams.

### Tighter Security, Less Risk

- Compromised systems were isolated fast, stopping attackers in their tracks.
- Blocking untrusted domains and restricting risky remote access tools made it harder for threats to get in.
- Clear, actionable security improvements ensured the company stayed protected moving forward.

## Conclusion

The series of targeted attacks by **Black Basta ransomware operators** served as a stark reminder of the vulnerabilities inherent in organizations, particularly among non-technical employees. The proactive measures taken by the UnderDefense team highlighted the **critical importance of robust security awareness training and effective communication protocols**. Continuous education and the implementation of technical safeguards are essential to protect against evolving threats.

Organizations must ensure that their **EDR solutions are effectively managed** and that employees are trained to recognize and report suspicious activities promptly. By fostering a culture of security awareness and vigilance, organizations can significantly reduce their risk of falling victim to social engineering attacks and other cyber threats.