**Cyber Threat Report**

**Threat Report ID:** UoL-CTI-25-0729  
**Date:** 29 July 2025  
**Reported by:** UoL Cyber Threat Intelligence Group  
**Threat level:** High

**Summary**

A sophisticated phishing and ransomware campaign is currently targeting UK-based higher education institutions. The campaign, attributed to a financially motivated threat group known as **‘**Vulcan Hydra’, is designed to gain access to university networks, exfiltrate sensitive data and demand cryptocurrency payments for decryption.

**1. Threat actor profile**

* Name: Vulcan Hydra (suspected Eastern European origin)
* Motivation: Financial gain
* Tactics: Phishing, credential theft, lateral movement, data exfiltration, ransomware deployment
* History: Involved in similar campaigns targeting research institutions in 2023–2024

**2. Attack vector**

* Initial access  
  Phishing emails impersonating university HR departments. Subject lines reference updated payroll systems and require staff to verify details via a malicious link.
* Payload  
  Once credentials are entered, a dropper downloads HydraCrypt, a custom ransomware variant capable of:
  + encrypting shared drives and cloud-based repositories
  + stealing browser-saved credentials
  + disabling endpoint recovery tools.

**3. Indicators of Compromise (IOCs)**

* Malicious domains:
  + university-payroll-check[.]com
  + hrportal-verify[.]org
* IP addresses:
  + 185.203.119.74 (linked to previous HydraCrypt attacks)
  + 92.118.160.22 (command and control node)
* Hashes of detected payloads:
  + e3b0c44298fc1c149afbf4c8996fb924... (HydraCrypt v3.2 installer)
  + f2d5e8ff9ec11817f9a1283d736b0143... (phishing attachment .docm)

**4. Timeline of activity**

| **Date** | **Activity** |
| --- | --- |
| 12 July | First phishing email reported by a staff member |
| 14 July | Network scans from known Hydra IPs detected |
| 15 July | Two faculty accounts compromised |
| 16 July | Suspicious lateral movement observed on research subnet |
| 18 July | Ransom note detected in shared drive |

**5. Impact (observed at peer institution)**

* Partial data encryption of research archives
* Three-day outage of internal file-sharing systems
* Loss of six months of unbacked-up admin records
* £50,000 ransom demanded (not paid)

**6. Intelligence source assessment**

| **Source** | **Reliability** | **Confidence** |
| --- | --- | --- |
| Internal incident logs | High | High |
| UK NCSC advisory (13 July) | High | High |
| OSINT from sector forum | Moderate | Moderate |
| Vendor-provided threat feed | High | Moderate |

**7. Notes**

* No evidence of data being leaked on dark web forums (as of 28 July)
* Vulcan Hydra known to return to previously exploited targets
* HydraCrypt has evaded detection by at least two major antivirus engines