

Introduction

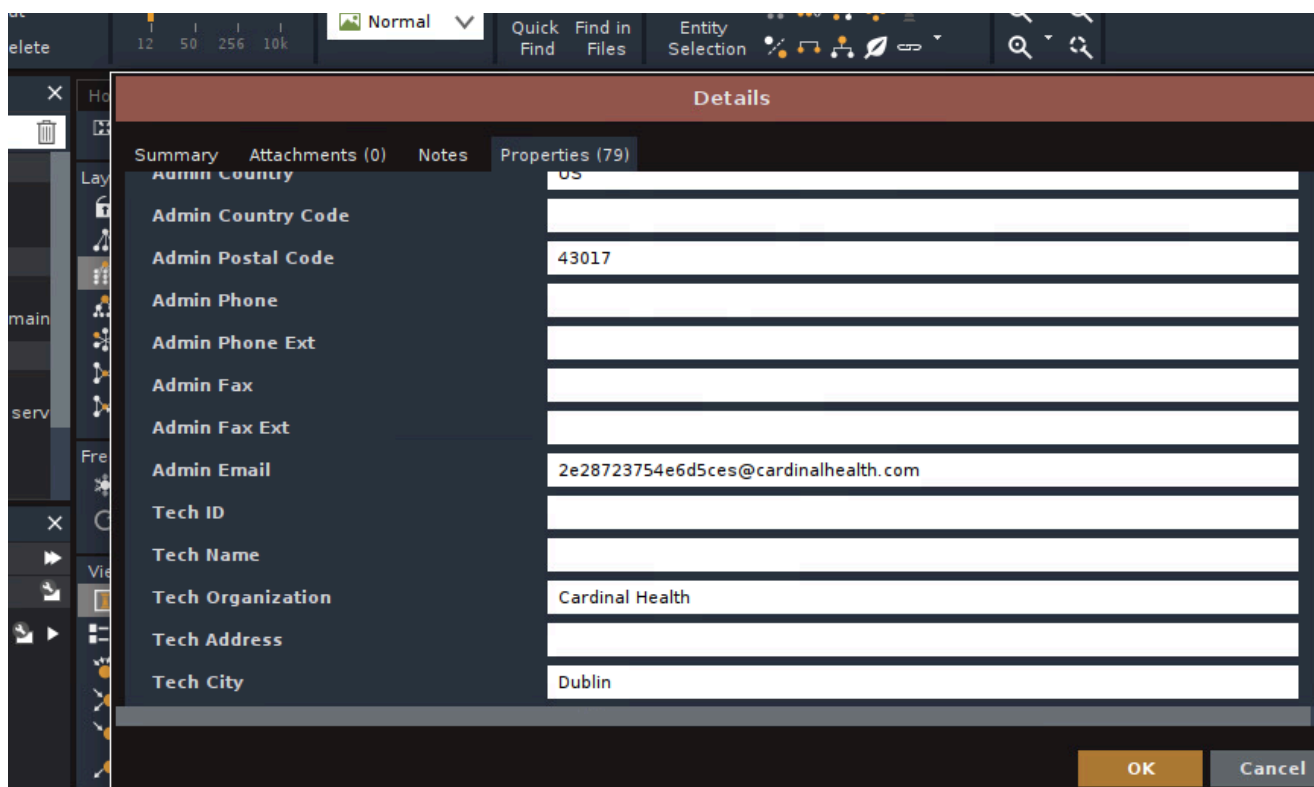
Cardinal Health is a global health care services and products company that provides customized solutions for hospitals, health systems, pharmacies, ambulatory surgery centers, clinical laboratories and physician offices worldwide. The company operates in two segments: Pharmaceutical and Medical. The company's website is <https://www.cardinalhealth.com/>.

Critical Information

Using the OSINT tool Maltego, I was able to find four critical pieces of information about Cardinal Health that could be valuable to an attacker:

1. Admin account email address

- The admin account email address.
- I used Maltego's **WhoisXML** transform to find this information from the company's domain name.
- This information could be used by an attacker to launch a **phishing** or **spear phishing** campaign, targeting the admin account with malicious emails that contain links or attachments that could compromise the account or the network. Alternatively, the attacker could try to **brute force** the password of the admin account or use **credential stuffing** techniques to gain access to the account and the company's systems.



The screenshot shows the Maltego interface with a 'Details' window open. The window has tabs for 'Summary', 'Attachments (0)', 'Notes', and 'Properties (79)'. The 'Properties' tab is active, displaying a list of fields and their values:

| Field | Value |
|--------------------|--------------------------------------|
| Admin Country | US |
| Admin Country Code | |
| Admin Postal Code | 43017 |
| Admin Phone | |
| Admin Phone Ext | |
| Admin Fax | |
| Admin Fax Ext | |
| Admin Email | 2e28723754e6d5ces@cardinalhealth.com |
| Tech ID | |
| Tech Name | |
| Tech Organization | Cardinal Health |
| Tech Address | |
| Tech City | Dublin |

At the bottom right of the window are 'OK' and 'Cancel' buttons.

2. Subdomains with restricted access

- There are a lot of subdomains that can be reached on the internet but they are forbidden from access, such as SMTP server, DNS servers, VPN servers, and virtual server on AWS.
- I used Maltego's **Shodan** transform to find these subdomains from the company's domain name.
- These subdomains could be used by an attacker to perform **reconnaissance** or **scanning** activities, looking for vulnerabilities or misconfigurations that could allow them to bypass the access restrictions and gain access to the company's internal network or resources. For example, the attacker could try to exploit a **DNS cache poisoning** attack, a **VPN tunnel hijacking** attack, or a **cloud misconfiguration** attack.

Note: please look at the attached maltego file

3. Email addresses of employees

- I found a lot of email addresses of employees who I think work at the company.
- I used Maltego's **To Email Address** transform to find these email addresses from the company's domain name.
- These email addresses could be used by an attacker to launch a **phishing** or **spear phishing** campaign, targeting the employees with malicious emails that contain links or attachments that could compromise their accounts or devices. Alternatively, the attacker could try to **brute force** the passwords of the employees' accounts or use **credential stuffing** techniques to gain access to their accounts and the company's data or systems.

Note: please look at the attached maltego file

4. Vulnerable medical devices

- I found a PDF document that describes a **security vulnerability** in some of the medical devices manufactured by Cardinal Health's subsidiary, Alaris. The document is dated **August 4, 2006** and is archived at this [link](#).
- I used Maltego's **wayback machine** transform to find this document from the company's domain name.
- The document states that some of the Alaris **infusion pumps** and **point-of-care units** have a **buffer overflow** vulnerability that could allow an attacker to execute **arbitrary code** on the devices. The document also provides a **patch** to fix the vulnerability and advises the customers to **update** their devices as soon as possible.
- This information could be used by an attacker to target the vulnerable medical devices and potentially **compromise** their functionality, **steal** sensitive patient data, or **cause** physical harm to the patients. The attacker could exploit the vulnerability by sending **malicious packets** to the devices over the network or by physically **accessing** the devices and inserting a **malicious device** into the serial port. The attacker could also try to **prevent** the customers from applying the patch or **reverse engineer** the patch to find the vulnerability.

Conclusion

In conclusion, Cardinal Health is a large and influential health care company that has a lot of sensitive and valuable information and assets. Using the OSINT tool Maltego, I was able to find three critical pieces of information that could be exploited by an attacker to compromise the company's security and privacy. Therefore, Cardinal Health should implement strong security measures and policies to protect its domain name, subdomains, email accounts, and network from potential attacks.