**BÁO CÁO TUẦN**

**Kết quả Giám sát ATTT Hệ thống**

**{{ organization.name }}**

**{{ date\_now }}**

**CyRadar Threat Intelligence Platform**

**BÁO CÁO TUẦN**

**Kết quả Giám sát ATTT Hệ thống**

**{{organization.name}}**

|  |  |
| --- | --- |
| **Đơn vị được giám sát** | {{ organization.name }} |
| **Địa chỉ** | {{ organization.address }} |
| **Thời gian giám sát** | {{ organization.execution\_time.start\_time }} – {{ organization.execution\_time.end\_time }} |
| **Đơn vị triển khai** | Công ty Cổ phần An toàn Thông tin CyRadar |
| **Phân loại tài liệu** | Giới hạn |

**MỤC LỤC**

[TỔNG QUAN 4](#_Toc201249766)

[KHUYẾN NGHỊ KHẮC PHỤC 7](#_Toc201249767)

[PHỤ LỤC 8](#_Toc201249768)

[PHỤ LỤC 1. TÀI SẢN GIÁM SÁT 8](#_Toc201249769)

[PHỤ LỤC 2. CỔNG DỊCH VỤ ĐANG MỞ 9](#_Toc201249770)

[PHỤ LỤC 3. NGUY CƠ, ĐIỂM YẾU TRÊN CÁC TÀI SẢN SỐ 10](#_Toc201249771)

[PHỤ LỤC 4. LỘ LỌT TÀI KHOẢN 12](#_Toc201249772)

[PHỤ LỤC 5. LỘ LỌT THÔNG TIN THẺ TÍN DỤNG 13](#_Toc201249773)

[PHỤ LỤC 6. LỘ LỌT TÀI LIỆU 14](#_Toc201249774)

[PHỤ LỤC 7. LẠM DỤNG THƯƠNG HIỆU 16](#_Toc201249775)

[PHỤ LỤC 8. YÊU CẦU ĐIỀU TRA 17](#_Toc201249776)

[PHỤ LỤC 9. IP LIÊN QUAN MÃ ĐỘC/BOTNET 18](#_Toc201249777)

[PHỤ LỤC 10. CHIẾN DỊCH TẤN CÔNG 19](#_Toc201249778)

TỔNG QUAN

Hệ thống CyRadar Threat Intelligence thực hiện giám sát tài sản của {{organization.name}} nhằm đưa ra các cảnh báo về nguy cơ an ninh mạng trong hệ thống khách hàng.

Báo cáo này bao gồm kết quả giám sát đánh giá về các nguy cơ, mô tả chi tiết các vấn đề đã phát hiện cùng các khuyến nghị để xử lý khắc phục vấn đề.

**Thông tin tổng quan**

|  |  |  |
| --- | --- | --- |
| {%tr for i in range(0, overview.overview.density|length, 3) %} | | |
| {%tc for item in overview.overview.density[i:i+3] %} | {{item}} | {%tc endfor %} |
| {%tr endfor %} | | |

**{% if overview.chart.dl\_credential.domain %}**

**Lộ lọt tài khoản**

**{{p overview.chart.chart\_credential\_domain}}**

**{% endif %}**

**Lỗ hổng bảo mật**

**Lộ lọt tài liệu**

KHUYẾN NGHỊ KHẮC PHỤC

**{%- if overview.overview.risk %}**

**Lỗ hổng bảo mật**

* Cập nhật bản vá mới nhất từ nhà cung cấp
* Đối với lỗ hổng nguy hiểm, nếu chưa thể vá, tạm thời vô hiệu hóa tính năng chứa lỗ hổng
* Tăng cường bảo vệ và giám sát bằng Firewall, IDS/IPS, SIEM…
* Ghi log đầy đủ và lưu trữ để phục vụ điều tra sau này
* Kiểm tra lại hệ thống sau xử lý để đảm bảo an toàn

{%- endif %}

**{%- if overview.overview.dl\_credential or overview.overview.dl\_credit\_card or overview.overview.dl\_document %}**

**Lộ lọt dữ liệu (thông tin tài khoản, tài liệu, thẻ tín dụng)**

* Xác minh dữ liệu bị lộ lọt
* Xử lý khắc phục tùy loại dữ liệu: đổi mật khẩu, vô hiệu hóa API key, khóa thẻ tín dụng, xử lý sự cố truyền thông, thông báo tới khách hàng…
* Khoanh vùng, điều tra nguyên nhân lộ lọt
* Rà soát, làm sạch nguy cơ gây lộ lọt trong hệ thống
* Tăng cường áp dụng các chính sách về ATTT trong nội bộ (phân quyền truy cập, yêu cầu bật xác thực đa lớp, định kỳ đổi mật khẩu, sử dụng phần mềm chống mã độc…)

{%- endif %}

**{%- if overview.overview.brand\_abuse %}**

**Bị lạm dụng thương hiệu**

* Thông báo tới khách hàng của tổ chức không truy cập vào các tên miền/đường dẫn lừa đảo
* Phối hợp với các cơ quan chức năng để ngăn chặn các tên miền lừa đảo

{%- endif %}

**{%- if overview.overview.campaign\_botnet or overview.overview.campaign\_campaign %}**

**Liên quan Malware/Botnet**

* Xác định và cách ly hệ thống bị nghi nhiễm khỏi mạng nội bộ
* Thu thập logs & dấu vết (IOC) phục vụ điều tra
* Quét toàn bộ hệ thống bằng công cụ Antivirus/EDR và thực hiện rà soát thủ công bằng chuyên gia để đảm bảo phát hiện, gỡ bỏ hoàn toàn mã độc
* Thay đổi mật khẩu của các tài khoản liên quan
* Điều tra đường tấn công, và khắc phục vấn đề
* Giám sát hoạt động mạng chặt chẽ sau khi xử lý

{%- endif %}

PHỤ LỤC

PHỤ LỤC 1. TÀI SẢN GIÁM SÁT

**{% for domain in appendix.asset.domain\_ip %}**

**{{ domain.group }}**

| **#** | **Tài sản** | **Mô tả** |
| --- | --- | --- |
| {%tr for item in domain.assets %} | | |
| {{loop.index}} | {{ item.value }} | {{ item.description }} |
| {%tr endfor %} | | |

**{% endfor %}**

**Thông tin sản phẩm**

| **#** | **Tài sản** | **Mô tả** |
| --- | --- | --- |
| {%tr for item in appendix.asset.products %} | | |
| {{loop.index}} | {{ item.value }} | {{ item.description }} |
| {%tr endfor %} | | |

**Thông tin định danh**

| **#** | **Tài sản** | **Loại** |
| --- | --- | --- |
| {%tr for item in appendix.asset.identify %} | | |
| {{loop.index}} | {{ item.value }} | {{ item.description }} |
| {%tr endfor %} | | |

{%- if appendix.open\_port %}

PHỤ LỤC 2. CỔNG DỊCH VỤ ĐANG MỞ

| **#** | **IP** | **Port** | **Dịch vụ** | **Phiên bản** |
| --- | --- | --- | --- | --- |
| {%tr for item in appendix.asset.open\_port %} | | | | |
| {{loop.index}} | {{ item.ip }} | {{ item.port }} | {{ item.service }} | {{ item.vervion }} |
| {%tr endfor %} | | | | |

{%- endif %}

PHỤ LỤC 3. NGUY CƠ, ĐIỂM YẾU TRÊN CÁC TÀI SẢN SỐ

{%- if appendix.vulnerability.cve %}

1. CÁC SẢN PHẨM, PHẦN MỀM ỨNG DỤNG

| **#** | **Sản phẩm** | **Điểm yếu, lỗ hổng** | **Mức độ** | **Mô tả** | **Khuyến nghị** |
| --- | --- | --- | --- | --- | --- |
| {%tr for item in appendix.vulnerability.cve %} | | | | | |
| {{loop.index}} | {{item.product.name}} | {% for v in item.product.cves %} | | | |
| {{v.name}} | **{%- if v.severity == ‘critical’ -%}Nghiêm trọng{%- elif v.severity == ‘high’ -%}Cao{%- elif v.severity == ‘medium’ -%}Trung bình{%- elif v.severity == ‘low’ -%}Thấp{%- elif v.severity == ‘info’ -%}Thông tin{%- else -%}None{%- endif -%}** | {{ v.description }} | {{ v.recommendation }} |
| {% endfor %} | | | |
| {%tr endfor %} | | | | | |

{%- endif %}

1. CÁC IP/DOMAIN

| **#** | **Host** | **Nguy cơ** | **Mức độ** | **Mô tả** | **Khuyến nghị** |
| --- | --- | --- | --- | --- | --- |
| 1 | 103.178.214.175 | Liferay Portal 7.3.3 < 7.4.3.17 SQLi Vulnerability | **Cao** | Liferay Portal tồn tại lỗ hổng SQL injection (SQLi).  Lỗ hổng SQL injection trong quá trình nâng cấp PortletPreferences của mô-đun Fragment cho phép kẻ tấn công thực thi các lệnh SQL tùy ý thông qua thuộc tính 'namespace' của PortletPreferences. | Cập nhật lên phiên bản 7.4.3.17 trở lên. |
| SMB Brute Force Logins With Default Credentials | **Nghiêm trọng** | Một số thông tin xác thực mặc định đã biết được thử nghiệm để đăng nhập qua giao thức SMB. | Thay đổi mật khẩu càng sớm càng tốt. |

PHỤ LỤC 4. LỘ LỌT TÀI KHOẢN

| **#** | **Đường dẫn** | **Tên đăng nhập** | **Mật khẩu** | **Thời gian ghi nhận** |
| --- | --- | --- | --- | --- |
| 1 | <https://elearning.evn.com.vn> | [Fa3805nlyca@vodafone.de](mailto:Fa3805nlyca@vodafone.de) | Q\*\*\*\*\*\*\*\*\*4 | 13/06/2025 |
| 2 | <https://domain.com> | User123 | Q\*\*\*\*\*\*\*\*\*4 | 13/06/2025 |
| 3 | <https://domain.com>/login | Admin | Q\*\*\*\*\*\*\*\*\*4 | 13/06/2025 |
| 4 | <https://domain.com> | Demo2 | Q\*\*\*\*\*\*\*\*\*4 | 13/06/2025 |

PHỤ LỤC 5. LỘ LỌT THÔNG TIN THẺ TÍN DỤNG

| **#** | **Số thẻ** | **Ngày hết hạn** | **Thời gian ghi nhận** |
| --- | --- | --- | --- |
| 1 | 5608361254865243 | 12/12 | 13/06/2025 |
| 2 | 5608361254865243 | 02/24 | 13/06/2025 |
| 3 | 5608361254865243 | N/A | 13/06/2025 |

PHỤ LỤC 6. LỘ LỌT TÀI LIỆU

| **#** | **Tên tài liệu** | **Kích thước** | **Đường dẫn** | **Thời gian ghi nhận** |
| --- | --- | --- | --- | --- |
| 1 | Test.txt | 12KB | <https://github.com/phamleduy04>/test/txt | 13/06/2025 |
| 2 | Hopdongabc.docx | 53KB | https://github.com/phamleduy04/hopdongabc.docx | 13/06/2025 |

PHỤ LỤC 7. LẠM DỤNG THƯƠNG HIỆU

| **#** | **Tên** | **Mô tả** | **Thời gian ghi nhận** |
| --- | --- | --- | --- |
| 1 | Sevenlog.com | Tên miền thực hiện giả lập website abc | 13/06/2025 |
| 2 | Drawebvd.uk | Tên miền thực hiện giả lập website abc | 13/06/2025 |
| 3 | Daivents-net.ga | Tên miền thực hiện giả lập website abc | 13/06/2025 |

PHỤ LỤC 8. YÊU CẦU ĐIỀU TRA

| **#** | **Tên miền** | **Trạng thái** | **Thời gian yêu cầu** | **Thời gian hoàn thành** |
| --- | --- | --- | --- | --- |
| 1 | Test.com | Hoàn thành | 13/06/2025 | 13/06/2025 |
| 2 | Domain.test | Đang xử lý | 13/06/2025 | 13/06/2025 |
| 3 | Test-domain.com | Từ chối | 13/06/2025 | 13/06/2025 |

PHỤ LỤC 9. IP LIÊN QUAN MÃ ĐỘC/BOTNET

| **#** | **IP** | **Thời gian ghi nhận** | **Thông tin bổ sung** |
| --- | --- | --- | --- |
| 1 | 134.93.49.75 | 13/06/2025 |  |
| 2 | 134.93.49.75 | 13/06/2025 |  |
| 3 | 134.93.49.75 | 13/06/2025 |  |

PHỤ LỤC 10. CHIẾN DỊCH TẤN CÔNG

(Các chiến dịch có thể ảnh hưởng đến tổ chức)

| **#** | **Tên chiến dịch** | **Mục tiêu** | | **Thời gian ghi nhận** |
| --- | --- | --- | --- | --- |
| **Quốc gia** | **Lĩnh vực** |
| 1 | APT28 | Việt Nam, Thái Lan | Tài chính | 13/06/2025 |
| 2 | [dr.compress@bk.ru](mailto:dr.compress@bk.ru) | N/A | N/A | 13/06/2025 |