**BÁO CÁO TUẦN**

**Kết quả Giám sát ATTT Hệ thống**

**dev**

**06-2025**

**CyRadar Threat Intelligence Platform**

**BÁO CÁO TUẦN**

**Kết quả Giám sát ATTT Hệ thống**

**dev**

|  |  |
| --- | --- |
| **Đơn vị được giám sát** | dev |
| **Địa chỉ** | Hanoi |
| **Thời gian giám sát** | 1970-01-02 17:17:36 – 1970-05-24 04:17:36 |
| **Đơn vị triển khai** | Công ty Cổ phần An toàn Thông tin CyRadar |
| **Phân loại tài liệu** | Giới hạn |

**MỤC LỤC**

[TỔNG QUAN 4](#_Toc201590037)

[KHUYẾN NGHỊ KHẮC PHỤC 7](#_Toc201590038)

[PHỤ LỤC 9](#_Toc201590039)

[PHỤ LỤC 1. TÀI SẢN GIÁM SÁT 9](#_Toc201590040)

[PHỤ LỤC 2. CỔNG DỊCH VỤ ĐANG MỞ 11](#_Toc201590041)

[PHỤ LỤC 3. NGUY CƠ, ĐIỂM YẾU TRÊN CÁC TÀI SẢN SỐ 13](#_Toc201590042)

[PHỤ LỤC 4. LỘ LỌT TÀI KHOẢN 15](#_Toc201590043)

[PHỤ LỤC 5. LỘ LỌT THÔNG TIN THẺ TÍN DỤNG 16](#_Toc201590044)

[PHỤ LỤC 6. LỘ LỌT TÀI LIỆU 17](#_Toc201590045)

[PHỤ LỤC 7. LẠM DỤNG THƯƠNG HIỆU 18](#_Toc201590046)

[PHỤ LỤC 8. YÊU CẦU ĐIỀU TRA 20](#_Toc201590047)

[PHỤ LỤC 9. IP LIÊN QUAN MÃ ĐỘC/BOTNET 21](#_Toc201590048)

[PHỤ LỤC 10. CHIẾN DỊCH TẤN CÔNG 22](#_Toc201590049)

TỔNG QUAN

Hệ thống CyRadar Threat Intelligence thực hiện giám sát tài sản của dev 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**

|  |  |
| --- | --- |
| Nguy cơ115% | Lộ lọt tài khoản115% |

**Lộ lọt tài khoản**

**Lỗ hổng bảo mật**

|  |  |  |
| --- | --- | --- |
| **Mức độ** | **Phát hiện** | **Biểu đồ** |
| **Nghiêm trọng** | 4 |  |
| **Cao** | 1 |
| **Trung bình** | 1 |
| **Thấp** | 1 |
| **Thông tin** | 1 |

**Lộ lọt tài liệu**

KHUYẾN NGHỊ KHẮC PHỤC

**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

PHỤ LỤC

## TÀI SẢN GIÁM SÁT

**Trung tâm Dữ liệu (TTDL)**

| **#** | **Tài sản** | **Mô tả** |
| --- | --- | --- |
| 1 | domain-test.com | description |
| 2 | domain-test.com | description |

**Trung tâm Dữ liệu (TTDL)**

| **#** | **Tài sản** | **Mô tả** |
| --- | --- | --- |
| 1 | domain-test.com | description |
| 2 | domain-test.com | description |

**Thông tin sản phẩm**

| **#** | **Tài sản** | **Mô tả** |
| --- | --- | --- |
| 1 | product1 | description |

**Thông tin định danh**

| **#** | **Tài sản** | **Loại** |
| --- | --- | --- |
| 1 | product1 | description |

CỔNG DỊCH VỤ ĐANG MỞ

| **#** | **IP** | **Port** | **Dịch vụ** | **Phiên bản** |
| --- | --- | --- | --- | --- |
| 1 | 1.1.1.1 | 2000 | ftp | 123 |

NGUY CƠ, ĐIỂM YẾU TRÊN CÁC TÀI SẢN SỐ

A.CÁC SẢN PHẨM, PHẦN MỀM ỨNG DỤNG

| **#** | **Sản phẩm** | **Điểm yếu, lỗ hổng** | **Mức độ** | **Mô tả** | **Khuyến nghị** |
| --- | --- | --- | --- | --- | --- |
| 1 | dev | CVE-2020-2020 | **Nghiêm trọng** | description | update to version 1.0.1 |
| CVE-2020-2022 | **Nghiêm trọng** | description | update to version 1.0.1 |

B.CÁC IP/DOMAIN

| **#** | **Host** | **Nguy cơ** | **Mức độ** | **Mô tả** | **Khuyến nghị** |
| --- | --- | --- | --- | --- | --- |
| 1 | 1.1.1.1 | CVE-2020-2020 | **Nghiêm trọng** | description | update to version 1.0.1 |

LỘ LỌT TÀI KHOẢN

| **#** | **Đường dẫn** | **Tên đăng nhập** | **Mật khẩu** | **Thời gian ghi nhận** |
| --- | --- | --- | --- | --- |
| 1 | path/to/credential1 | username1 | password1 | 1234567890 |
| 2 | path/to/credential1 | username1 | password1 | 1234567890 |

LỘ LỌT THÔNG TIN THẺ TÍN DỤNG

| **#** | **Số thẻ** | **Chủ thẻ** | **Ngày hết hạn** | **Thời gian ghi nhận** |
| --- | --- | --- | --- | --- |
| 1 | 1234-5678-9012-3456 | thangnx | 12/25 | 1234567890 |
| 2 | 1234-5678-9012-3456 | thangnx | 12/25 | 1234567890 |

LỘ LỌT TÀI LIỆU

| **#** | **Tên tài liệu** | **Kích thước** | **Đường dẫn** | **Thời gian ghi nhận** |
| --- | --- | --- | --- | --- |
| 1 | file1.docx | 123456 | path/to/file1.docx | 1234567890 |
| 2 | file2.docx | 123456 | path/to/file2.docx | 1234567890 |

LẠM DỤNG THƯƠNG HIỆU

| **#** | **Tên** | **Mô tả** | **Thời gian ghi nhận** |
| --- | --- | --- | --- |
| 1 | abuse-domain.com | phishing | 1234567890 |
| 2 | abuse-domain1.com | phishing | 1234567890 |

YÊU CẦU ĐIỀU TRA

| **#** | **Tên miền** | **Trạng thái** | **Thời gian yêu cầu** | **Thời gian hoàn thành** |
| --- | --- | --- | --- | --- |
| 1 |  |  | 1234567890 |  |
| 2 |  |  | 1234567890 |  |

IP LIÊN QUAN MÃ ĐỘC/BOTNET

| **#** | **IP** | **Thời gian ghi nhận** | **Thông tin bổ sung** |
| --- | --- | --- | --- |
| 1 | 1.1.1.1 | 1234567890 | Botnet detected |
| 2 | 1.1.1.2 | 1234567890 | Botnet detected |

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 | Campaign 1 | Description of Campaign 1 | Technology | 1234567890 |
| 2 | Campaign 2 | Description of Campaign 2 | Finance | 1234567890 |