hpt knowing IT

HSOC HPT Product

BÁO CÁO AN NINH MẠNG

TOÀN CẢNH AN NINH MẠNG TRONG 6 THÁNG ĐẦU NĂM 2026

Xu hướng tấn công và quan sát thực tế từ
Trung tâm Giám sát An ninh mạng HPT

Tổng hợp xu hướng tấn công, quan sát thực tế từ hoạt động giám sát và các khuyến nghị ưu tiên dành cho doanh nghiệp

KỲ BÁO CÁO
Tháng 1 - tháng 6/2026

ĐƠN VỊ THỰC HIỆN
TRUNG TÂM GIÁM SÁT AN NINH MẠNG HPT - HSOC

https://hpt.vn/

MỤC LỤC

I. Tóm tắt

Trong sáu tháng đầu năm 2026, bức tranh an ninh mạng tiếp tục diễn biến phức tạp với sự kết hợp giữa khai thác lỗ hổng, đánh cắp danh tính, tấn công chuỗi cung ứng, mã độc, ransomware và các hoạt động gián điệp có chủ đích.

Thông qua dữ liệu tình báo an ninh mạng và quá trình giám sát liên tục tại nhiều môi trường doanh nghiệp, Trung tâm giám sát An ninh mạng HPT (HSOC) nhận thấy các tác nhân đe dọa đang tập trung vào năm điểm yếu chính:

- Các dịch vụ và thiết bị kết nối trực tiếp với Internet.
- Tài khoản người dùng và tài khoản đặc quyền.
- Máy chủ web, ứng dụng nghiệp vụ và hệ thống quản trị.
- Thiết bị đầu cuối và công cụ truy cập từ xa.
- Dữ liệu trên môi trường cộng tác, lưu trữ đám mây và SaaS.

Các quan sát thực tế cho thấy nhiều cuộc tấn công không bắt đầu bằng mã độc phức tạp. Chúng thường khởi đầu từ những dấu hiệu tưởng như thông thường: một lần đăng nhập từ vị trí hiếm khi xuất hiện, nhiều yêu cầu xác thực thất bại, một công cụ điều khiển từ xa xuất hiện trên máy chủ, truy vấn DNS tới tên miền đáng ngờ hoặc lưu lượng dò quét cổng mạng từ một thiết bị nội bộ.

Nếu không được phát hiện và xác minh kịp thời, những dấu hiệu này có thể phát triển thành các hành động xâm nhập trái phép, đánh cắp thông tin xác thực, di chuyển ngang, rò rỉ dữ liệu hoặc ransomware.

01	02	03	04	05
Internet-facing	Identity	Web & App	Endpoint	SaaS Data

Trong năm 2026, khả năng phát hiện sớm chuỗi hành vi bất thường quan trọng hơn việc chỉ phát hiện một mẫu mã độc riêng lẻ.

Điều này đòi hỏi SOC phải liên kết dữ liệu từ mạng, endpoint, danh tính, cloud và threat intelligence để nhận diện đúng bản chất rủi ro trước khi các tín hiệu riêng lẻ phát triển thành sự cố nghiêm trọng.

II. Phạm vi và phương pháp tổng hợp

Báo cáo được xây dựng từ ba nhóm nguồn chính:

1. Các bản tin tình báo an ninh mạng và cảnh báo lỗ hổng trong khoảng thời gian từ tháng 1 đến tháng 6 năm 2026.
2. Các báo cáo về chiến dịch tấn công, ransomware, APT và tấn công chuỗi cung ứng.
3. Dữ liệu case giám sát an toàn thông tin được các chuyên gia An toàn thông tin HPT - HSOC ghi nhận tại các môi trường doanh nghiệp.

Tập dữ liệu giám sát được rà soát bao gồm **bản ghi cảnh báo và trường hợp bất thường**. Trong đó, nhiều trường hợp được xác minh là hoạt động hợp lệ, nhưng cũng ghi nhận hàng trăm trường hợp có dấu hiệu tấn công, mã độc, truy cập đáng ngờ hoặc vi phạm chính sách cần được điều tra và xử lý.

Để bảo đảm tính bảo mật, toàn bộ thông tin nhận dạng đã được loại bỏ hoặc khái quát hóa. Báo cáo không công bố tên tổ chức, tài khoản, địa chỉ mạng, tên máy chủ, tên miền nội bộ hoặc cấu hình kỹ thuật riêng của bất kỳ khách hàng nào.

SECTION 1

Thiết bị biên và dịch vụ công khai tiếp tục là cửa ngõ xâm nhập chính

VPN, firewall, gateway, web server và các dịch vụ quản trị công khai vẫn là lớp rủi ro đầu tiên cần được kiểm soát.

Trong nửa đầu năm 2026, các nhóm tấn công tiếp tục nhắm vào VPN, firewall, gateway, máy chủ web, hệ thống quản trị và các ứng dụng công khai trên Internet.

Các cảnh báo đáng chú ý liên quan đến nhiều nền tảng phổ biến như Fortinet, Palo Alto Networks, Check Point, Citrix, Cisco, VMware, Veeam, SolarWinds, SAP và các nền tảng tự động hóa.

Chiến dịch FortiBleed là một ví dụ điển hình. Thay vì chỉ dựa trên một lỗ hổng zero-day mới, chiến dịch tận dụng khối lượng lớn thông tin xác thực đã bị đánh cắp hoặc rò rỉ trước đó để thử đăng nhập vào các thiết bị FortiGate và dịch vụ VPN trên toàn cầu.

Điều này phản ánh một xu hướng quan trọng: ngay cả khi thiết bị đã được vá, doanh nghiệp vẫn có thể bị xâm nhập nếu mật khẩu, token hoặc thông tin xác thực cũ chưa được thu hồi.

1.1 Quan sát thực tế từ hoạt động giám sát của HSOC

Trong các môi trường được giám sát, HSOC ghi nhận nhiều nhóm hành vi liên quan đến bề mặt tấn công Internet:

- Lưu lượng kết nối từ bên ngoài tới các cổng quản trị và dịch vụ nhạy cảm.
- Nhiều lần thử xác thực vào firewall, VPN hoặc hệ thống từ xa.
- Hoạt động quét cổng và dò tìm dịch vụ trên các địa chỉ công khai.
- Yêu cầu khai thác lỗ hổng nhằm vào máy chủ web và ứng dụng.
- Các mẫu truy cập tự động tìm kiếm giao diện quản trị, đường dẫn nhạy cảm và phiên bản phần mềm.
- Dịch vụ không cần thiết vẫn được công khai trên Internet.
- Lưu lượng khai thác nhắm vào camera, DVR, ứng dụng web và các thành phần middleware.

Một số hành vi đã bị firewall hoặc WAF chặn. Tuy nhiên, HSOC cũng ghi nhận những trường hợp kết nối được thiết lập thành công và cần phối hợp xác minh để phân biệt giữa hoạt động quản trị hợp lệ và truy cập trái phép.

1.2 Nguy cơ đối với doanh nghiệp

> ⚠ **Khi thiết bị biên hoặc dịch vụ công khai bị chiếm quyền, kẻ tấn công có thể đi thẳng từ lớp ngoài vào mạng nội bộ.**
>
> Rủi ro lớn nhất thường không nằm ở bản thân lỗ hổng kỹ thuật. Nó đến từ những thông tin xác thực cũ, cấu hình quản trị và dịch vụ không cần thiết vẫn tồn tại trên Internet, tạo điều kiện cho truy cập trái phép, duy trì hiện diện và triển khai ransomware.

Nếu thiết bị biên hoặc dịch vụ Internet-facing bị chiếm quyền, kẻ tấn công có thể:

- Vượt qua các lớp phòng vệ bên ngoài.
- Truy cập trực tiếp vào mạng nội bộ.
- Thu thập thông tin về kiến trúc và tài sản của doanh nghiệp.
- Đánh cắp cấu hình, mật khẩu và khóa truy cập.
- Tạo tài khoản quản trị hoặc cơ chế duy trì quyền truy cập.
- Sử dụng thiết bị làm điểm trung chuyển vào các vùng mạng khác.
- Vô hiệu hóa log hoặc thay đổi chính sách bảo mật.
- Triển khai mã độc và ransomware.

1.3 Khuyến nghị cho doanh nghiệp

Doanh nghiệp cần duy trì danh mục đầy đủ về toàn bộ tài sản Internet-facing và kiểm tra định kỳ:

- Cổng và dịch vụ đang công khai.
- Phiên bản hệ điều hành và firmware.
- Giao diện quản trị có thể truy cập từ Internet.
- Tài khoản cục bộ và tài khoản nhà cung cấp.
- Chứng thư số và thông tin xác thực đã hết hạn hoặc bị lộ.
- Thiết bị không còn được nhà sản xuất hỗ trợ.

Các giao diện quản trị nên được giới hạn bằng allowlist, bastion host hoặc VPN quản trị riêng. Tài khoản đặc quyền cần sử dụng MFA chống phishing và được tách khỏi tài khoản làm việc hằng ngày.

SECTION 2

Tấn công ứng dụng web và khai thác lỗ hổng vẫn diễn ra với tần suất cao

Ứng dụng nghiệp vụ và máy chủ web tiếp tục là nhóm tài sản bị thăm dò, khai thác và kiểm thử tự động trên diện rộng.

Dữ liệu giám sát cho thấy máy chủ web và ứng dụng nghiệp vụ tiếp tục là một trong những nhóm tài sản bị thăm dò thường xuyên nhất.

Các kỹ thuật được quan sát bao gồm:

- Quét thư mục và đường dẫn ẩn.
- Tìm kiếm trang quản trị.
- SQL injection.
- Path traversal.
- Thử khai thác remote code execution.
- Dò tìm phiên bản framework và middleware.
- Khai thác cấu hình mặc định.
- Thử truy cập tệp cấu hình, tệp sao lưu và thông tin nhạy cảm.
- Brute force vào giao diện quản trị ứng dụng.

Các hoạt động này thường được thực hiện tự động trên diện rộng. Tuy nhiên, nếu một mục tiêu phản hồi tích cực, kẻ tấn công có thể chuyển sang khai thác có chủ đích.

2.1 Quan sát thực tế từ HSOC

HSOC ghi nhận nhiều cảnh báo WAF, IDS và IPS liên quan đến yêu cầu khai thác ứng dụng web. Một số trường hợp đáng chú ý gồm:

- Chuỗi yêu cầu có dấu hiệu SQL injection.
- Hoạt động quét bằng công cụ tự động nhằm tìm endpoint và thư mục nhạy cảm.
- Yêu cầu khai thác nhắm vào framework hoặc máy chủ ứng dụng phổ biến.
- Truy cập bất thường tới giao diện quản trị.
- Lưu lượng khai thác lỗ hổng thực thi mã từ xa trên thiết bị hoặc ứng dụng công khai.
- Nhiều yêu cầu từ các địa chỉ khác nhau nhưng sử dụng chung mẫu khai thác.
- Tệp nén hoặc tệp thực thi xuất hiện trong thư mục ứng dụng web.

Một số tệp nén trong thư mục web sau đó được xác minh là phục vụ triển khai hợp lệ. Tuy nhiên, đây vẫn là hành vi cần giám sát vì kẻ tấn công thường sử dụng tệp nén để tập kết công cụ, dữ liệu đánh cắp hoặc webshell.

2.2 Bài học rút ra

✓ **Cảnh báo từ WAF chỉ là điểm bắt đầu; kết luận rủi ro cần dựa trên log máy chủ, endpoint và kết nối outbound.**

Một cảnh báo riêng lẻ chưa đủ để kết luận hệ thống đã bị xâm nhập. SOC cần liên kết dữ liệu WAF với:

- Log của máy chủ web.
- Log của hệ điều hành.
- Tiến trình được thực thi.
- Tệp mới được tạo.
- Kết nối outbound sau thời điểm bị khai thác.
- Thay đổi tài khoản và quyền truy cập.
- Log của EDR hoặc XDR.

Nếu chỉ quan sát lưu lượng phía ngoài mà không có log máy chủ, doanh nghiệp khó xác định yêu cầu khai thác đã bị chặn hay đã thực thi thành công.

2.3 Khuyến nghị cho doanh nghiệp

- Thực hiện vá lỗi sớm nhất có thể đối với các lỗ hổng đang bị khai thác trong thực tế.
- Không chỉ dựa vào điểm CVSS để xác định mức độ ưu tiên; cần đánh giá rủi ro theo bối cảnh doanh nghiệp, bao gồm attack path, asset criticality và exploit status.
- Đưa thông tin Internet exposure và giá trị tài sản vào mô hình quản lý lỗ hổng.
- Thu thập đầy đủ log WAF, web server, endpoint và ứng dụng.
- Thiết lập File Integrity Monitoring cho thư mục web.
- Cảnh báo khi xuất hiện webshell, script, tệp thực thi hoặc tệp nén bất thường.
- Tách tài khoản dịch vụ ứng dụng khỏi tài khoản quản trị hệ thống.
- Kiểm thử khả năng ngăn chặn và phát hiện bằng mô phỏng tấn công định kỳ.

SECTION 3

Danh tính trở thành bề mặt tấn công trọng yếu

Tài khoản hợp lệ giúp kẻ tấn công hòa lẫn vào hoạt động bình thường và vượt qua nhiều cơ chế phát hiện truyền thống.

Tấn công danh tính tiếp tục tăng trong năm 2026 vì tài khoản hợp lệ giúp kẻ tấn công hoạt động giống người dùng thông thường và tránh nhiều cơ chế phát hiện truyền thống.

Các nguồn thông tin xác thực thường bị khai thác gồm:

- Infostealer trên máy tính cá nhân.
- Phishing giả trang đăng nhập Microsoft 365 hoặc Google Workspace.
- Cookie và session token.
- Mật khẩu bị tái sử dụng.
- Tài khoản nhà cung cấp hoặc đối tác.
- Tài khoản không còn sử dụng nhưng chưa bị vô hiệu hóa.
- Mật khẩu được lưu trong trình duyệt hoặc script.
- Tài khoản dịch vụ có quyền cao.

3.1 Quan sát thực tế từ HSOC

Trong quá trình giám sát và phân tích các hoạt động xác thực, HSOC ghi nhận nhiều hành vi đáng chú ý liên quan đến tài khoản người dùng và truy cập hệ thống, bao gồm:

- Đăng nhập cổng Microsoft 365 từ vị trí địa lý hiếm gặp.
- Nhiều lần đăng nhập thất bại đối với cùng một tài khoản.
- Một nguồn thực hiện xác thực thất bại với nhiều tài khoản.
- Brute force vào SSH hoặc dịch vụ truy cập từ xa.
- Đăng nhập thành công sau chuỗi xác thực thất bại.
- Tài khoản có quyền cao đăng nhập ngoài giờ làm việc.
- Tạo mới tài khoản Linux hoặc Windows.
- Thêm tài khoản vào nhóm đặc quyền.
- Cấu hình mật khẩu không hết hạn.
- Đăng nhập bằng tài khoản quản trị từ thiết bị hoặc địa chỉ chưa từng quan sát.

Không phải tất cả các trường hợp trên đều là tấn công. Nhiều hành vi được xác minh là thay đổi nội bộ hoặc hoạt động bảo trì. Tuy nhiên, chúng có đặc điểm tương đồng với kỹ thuật sử dụng tài khoản hợp lệ của kẻ tấn công.

3.2 Nguy cơ đối với doanh nghiệp

!

Khi tài khoản hợp lệ bị chiếm, ranh giới giữa người dùng thật và kẻ tấn công trở nên rất khó phân biệt.

Đây là lý do danh tính cần được xem như một lớp phòng thủ trọng yếu, không chỉ là cơ chế đăng nhập.

Khi chiếm được tài khoản hợp lệ, kẻ tấn công có thể:

- Đọc và gửi email dưới danh nghĩa người dùng.
- Đánh cắp dữ liệu từ SharePoint, OneDrive hoặc hệ thống SaaS.
- Thiết lập rule chuyển tiếp email.
- Thay đổi thông tin thanh toán.
- Truy cập VPN và mạng nội bộ.
- Tạo ứng dụng OAuth độc hại.
- Leo thang đặc quyền.
- Vô hiệu hóa phương thức MFA hoặc đăng ký thiết bị mới.
- Sử dụng tài khoản bị chiếm để phishing người dùng khác.

3.3 Khuyến nghị cho doanh nghiệp

Doanh nghiệp nên ưu tiên:

- Sử dụng MFA chống phishing như FIDO2 hoặc passkey.
- Conditional Access theo vị trí, trạng thái thiết bị và mức độ rủi ro.
- Privileged Access Management.
- Tài khoản quản trị riêng biệt.
- Vô hiệu hóa xác thực cũ.
- Giám sát hành vi đăng nhập bất thường.
- Tự động thu hồi token và session khi phát hiện nguy cơ.
- Xác minh ngoài băng đối với yêu cầu reset mật khẩu hoặc MFA.
- Kiểm tra tài khoản không hoạt động và tài khoản của nhân sự đã nghỉ việc.

SECTION 4

Mã độc và lưu lượng Command and Control (C2) vẫn tồn tại trong mạng doanh nghiệp

Các tín hiệu từ endpoint, DNS và kết nối outbound cần được tương quan để phát hiện chuỗi hành vi hậu khai thác.

Trong dữ liệu giám sát, HSOC ghi nhận nhiều trường hợp endpoint hoặc thiết bị nội bộ tạo kết nối tới địa chỉ, tên miền hoặc hạ tầng có dấu hiệu liên quan đến mã độc.

Các hành vi bao gồm:

- Truy vấn DNS tới tên miền đáng ngờ.
- Kết nối HTTP hoặc TCP tới hạ tầng Command and Control (C2).
- Phát hiện spyware, adware, dropper và cryptominer.
- Tệp có hash nằm trong danh sách mã độc.
- Tệp độc hại được tải lên nền tảng lưu trữ đám mây.
- Tiến trình khả nghi được thực thi từ thư mục người dùng hoặc thư mục công cộng.
- PowerShell tải và thực thi script từ Internet.
- Công cụ credential dumping xuất hiện trên endpoint.
- Tiến trình hệ thống hợp lệ bị lợi dụng để nạp mã độc.

4.1 Một chuỗi tấn công điển hình được HSOC phát hiện

Trong một trường hợp giám sát, HSOC ghi nhận một chuỗi hành vi có đầy đủ đặc điểm của một cuộc xâm nhập:

1. PowerShell thực thi script từ thư mục dùng chung.
2. Script kết nối tới nguồn bên ngoài để tải công cụ hậu khai thác.
3. Một tệp giả mạo ứng dụng hợp lệ thiết lập kết nối ngược.
4. Kẻ tấn công sử dụng kỹ thuật bypass UAC để nâng quyền.
5. DLL độc hại được nạp thông qua tiến trình hệ thống hợp lệ.
6. Công cụ thu thập thông tin xác thực được gọi qua PowerShell.
7. Lịch sử PowerShell và Windows Event Log bị xóa.
8. Dịch vụ mới được tạo nhằm thực thi lệnh.
9. Một tài khoản mới được thêm vào hệ thống.

Chuỗi hành vi được phát hiện và kích hoạt quy trình phản ứng sự cố trước khi ghi nhận tác động lớn hơn đến môi trường.

4.2 Ý nghĩa của case

CASE INSIGHT

Một chuỗi tấn công thực tế thường tạo ra nhiều tín hiệu nhỏ; giá trị của SOC là liên kết chúng thành một câu chuyện rủi ro có thể hành động.

Trường hợp trên cho thấy một cuộc tấn công thực tế hiếm khi chỉ tạo ra một cảnh báo. Nó thường gồm nhiều bước tương ứng với các giai đoạn MITRE ATT&CK:

- Execution.
- Persistence.
- Privilege Escalation.
- Defense Evasion.
- Credential Access.
- Command and Control.

Nếu các cảnh báo chỉ được xử lý riêng lẻ, đội ngũ vận hành có thể bỏ qua mối liên hệ giữa PowerShell, tạo dịch vụ, kết nối mạng, xóa log và tạo tài khoản.

4.3 Khuyến nghị cho doanh nghiệp

- Tương quan cảnh báo theo host, user và thời gian.
- Chặn PowerShell không cần thiết hoặc áp dụng Constrained Language Mode.
- Giám sát tiến trình từ thư mục Public, Temp và AppData.
- Phát hiện tải script và thực thi trực tiếp từ Internet.
- Cảnh báo việc xóa Windows Event Log.
- Giám sát tạo mới service, scheduled task và tài khoản.
- Chặn kết nối outbound tới cổng hoặc hạ tầng không được phê duyệt.
- Hạn chế công cụ quản trị có thể thực hiện credential dumping.
- Thu thập Sysmon hoặc telemetry tương đương trên máy chủ quan trọng.

SECTION 5

Công cụ điều khiển từ xa hợp pháp tạo ra điểm mù bảo mật

Công cụ hỗ trợ kỹ thuật có thể trở thành kênh duy trì truy cập nếu thiếu kiểm soát, danh sách phê duyệt và audit trail.

Các công cụ như UltraViewer, VNC, AnyDesk và các nền tảng Remote Monitoring and Management có thể được sử dụng hợp pháp để hỗ trợ kỹ thuật. Tuy nhiên, chúng cũng thường bị kẻ tấn công lợi dụng để duy trì quyền truy cập.

5.1 Quan sát thực tế từ HSOC

Trong quá trình giám sát và phân tích an toàn thông tin, các chuyên gia tại HSOC đã ghi nhận một số dấu hiệu đáng chú ý liên quan đến hoạt động truy cập từ xa trên các máy chủ, bao gồm:

- Công cụ remote lần đầu xuất hiện trên máy chủ.
- Dịch vụ VNC tự động khởi động ngoài giờ làm việc.
- Phiên Remote Desktop thành công ngoài khung giờ thông thường.
- Tệp được chuyển tới máy chủ thông qua phiên remote.
- Công cụ quản trị từ xa chạy dưới quyền SYSTEM hoặc Administrator.
- Công cụ remote xuất hiện trên máy chủ quan trọng nhưng không có thông tin change request tương ứng.

Một số trường hợp được xác minh là hoạt động hỗ trợ hoặc bảo trì hợp lệ. Dù vậy, việc thiếu danh sách công cụ được phê duyệt làm tăng thời gian xác minh và có thể che giấu hoạt động của kẻ tấn công.

5.2 Nguy cơ đối với doanh nghiệp

- Truy cập lâu dài mà không cần triển khai mã độc riêng.
- Vượt qua một số kiểm soát dựa trên chữ ký.
- Truyền tệp và thực thi lệnh từ xa.
- Khó phân biệt giữa IT support và tấn công.
- Kẻ tấn công sử dụng công cụ sẵn có để “blend in” với hoạt động quản trị.

5.3 Khuyến nghị cho doanh nghiệp

KIỂM SOÁT ƯU TIÊN

Danh sách công cụ remote được phê duyệt là điều kiện nền để phân biệt hỗ trợ kỹ thuật hợp lệ với truy cập trái phép.

Doanh nghiệp nên:

- Xây dựng allowlist công cụ remote được phê duyệt.
- Cấm công cụ remote không được quản lý trên máy chủ.
- Yêu cầu change request hoặc ticket trước khi truy cập.
- Giới hạn theo nhóm người dùng, thiết bị và khung giờ.
- Ghi hình hoặc lưu audit trail đối với phiên quản trị đặc quyền.
- Cảnh báo khi công cụ remote xuất hiện lần đầu.
- Tự động cô lập thiết bị nếu công cụ bị cấm được thực thi.

SECTION 6

Rò rỉ dữ liệu đang dịch chuyển sang SaaS và nền tảng cộng tác

Dữ liệu nhạy cảm có thể rời khỏi doanh nghiệp thông qua chia sẻ, tải xuống và ứng dụng cloud hợp pháp.

Khi doanh nghiệp sử dụng Microsoft 365, Google Workspace và các nền tảng lưu trữ đám mây, dữ liệu có thể bị rò rỉ mà không cần truyền qua cổng mạng truyền thống.

6.1 Quan sát thực tế từ HSOC

Các nhóm hành vi được ghi nhận bao gồm:

- Chia sẻ tệp với địa chỉ email bên ngoài.
- Tải xuống số lượng lớn tệp bởi cùng một tài khoản.
- Truyền dữ liệu dung lượng lớn tới một đích.
- Tệp mã độc được tải lên OneDrive.
- Hành vi truy cập hoặc tải dữ liệu khác biệt so với baseline của người dùng.
- Dữ liệu được nén trong thư mục ứng dụng hoặc thư mục dùng chung.

- Lưu lượng có dấu hiệu data staging trước khi truyền ra ngoài.

Một số trường hợp chia sẻ hoặc tải dữ liệu là hoạt động công việc hợp lệ. Tuy nhiên, khi tài khoản đã bị chiếm, chính các chức năng SaaS hợp pháp có thể được sử dụng để đánh cắp dữ liệu.

6.2 Nguy cơ đối với doanh nghiệp

> **!** **Dữ liệu có thể bị rò rỉ qua chính các chức năng chia sẻ và tải xuống hợp pháp của nền tảng SaaS.**

- Rò rỉ thông tin khách hàng.
- Mất dữ liệu cá nhân.
- Lộ hợp đồng, báo giá và tài liệu chiến lược.
- Đánh cắp mã nguồn hoặc tài sản trí tuệ.
- Vi phạm nghĩa vụ pháp lý và hợp đồng.
- Không phát hiện được sự cố nếu chỉ giám sát firewall.

6.3 Khuyến nghị cho doanh nghiệp

- Thu thập Microsoft 365 Unified Audit Log hoặc log SaaS tương đương.
- Giám sát chia sẻ tệp ra bên ngoài.
- Cảnh báo tải xuống số lượng lớn.
- Áp dụng nhãn phân loại dữ liệu và DLP.
- Kiểm soát ứng dụng OAuth.
- Thiết lập giới hạn chia sẻ theo nhóm dữ liệu.
- Liên kết hành vi dữ liệu với rủi ro đăng nhập của người dùng.
- Thu hồi phiên đăng nhập khi phát hiện hành vi bất thường.

SECTION 7

Tấn công chuỗi cung ứng làm gia tăng rủi ro từ phần mềm hợp lệ

Dependency, tài khoản nhà phát triển và pipeline CI/CD cần được xem là một phần của bề mặt tấn công mở rộng.

Các chiến dịch tấn công chuỗi cung ứng trong nửa đầu năm 2026 tiếp tục nhắm vào phần mềm, thư viện mã nguồn mở, tài khoản nhà phát triển và quy trình cập nhật.

Các trường hợp công khai đáng chú ý liên quan đến:

- Trình cập nhật phần mềm bị lợi dụng.
- Các gói npm và PyPI bị cài mã độc.
- Tài khoản nhà phát triển bị chiếm quyền.
- Thư viện giả mạo các dự án phổ biến.
- Website cung cấp phần mềm bị biến thành watering hole.
- Gói phần mềm đánh cắp token và biến môi trường CI/CD.

7.1 Nguy cơ đối với doanh nghiệp

Một thư viện độc hại có thể:

- Đánh cắp API key và access token.
- Truy cập kho mã nguồn.
- Can thiệp pipeline CI/CD.
- Đưa backdoor vào sản phẩm.
- Lây lan sang khách hàng.
- Tạo ra sự cố có quy mô chuỗi cung ứng.

Doanh nghiệp có thể bị ảnh hưởng thông qua dependency gián tiếp, ngay cả khi không chủ động cài đặt gói độc hại.

7.2 Khuyến nghị cho doanh nghiệp

- Duy trì Software Bill of Materials.
- Khóa phiên bản dependency.
- Kiểm tra hash và chữ ký.
- Quét dependency trong CI/CD.
- Bảo vệ tài khoản nhà phát triển bằng MFA chống phishing.
- Giảm quyền của token phát hành package.

- Không lưu secret trong source code.
- Giám sát hành vi bất thường trên hệ thống build.
- Luân chuyển token khi phát hiện dependency bị xâm nhập.

SECTION 8

Ransomware ưu tiên vô hiệu hóa hệ thống bảo mật và sao lưu

Phòng thủ ransomware cần tập trung vào các hành vi tiền mã hóa, khả năng phục hồi và bảo vệ hệ thống backup.

Ransomware hiện đại thường thực hiện đánh cắp dữ liệu trước khi mã hóa. Các nhóm tấn công cũng tập trung vô hiệu hóa EDR và phá hủy khả năng phục hồi. Kỹ thuật Bring Your Own Vulnerable Driver tiếp tục được sử dụng để khai thác driver hợp lệ nhưng tồn tại lỗ hổng, từ đó can thiệp vào kernel và chấm dứt tiến trình bảo mật.

Hệ thống backup cũng trở thành mục tiêu ưu tiên vì thường:

Điểm yếu backup	Rủi ro ransomware	Kiểm soát ưu tiên
Kết nối trực tiếp với production	Kẻ tấn công có thể xóa hoặc mã hóa bản sao lưu	Tách vùng, giới hạn truy cập, immutable backup
Tài khoản backup dùng chung	Leo thang quyền và phá hủy khả năng phục hồi	Tài khoản riêng, MFA, PAM
Chưa kiểm thử khôi phục	Không chắc chắn về RTO/RPO khi xảy ra sự cố	Diễn tập phục hồi định kỳ

- Chứa quyền truy cập tới nhiều máy chủ.
- Lưu thông tin xác thực.
- Có khả năng xóa hoặc thay đổi bản sao lưu.
- Được kết nối trực tiếp với môi trường production.

8.1 Liên hệ với dữ liệu giám sát

Các hành vi HSOC ghi nhận như xóa log, tải công cụ credential dumping, tạo service, tạo tài khoản, sử dụng công cụ remote và kết nối C2 đều có thể xuất hiện trong giai đoạn chuẩn bị của một cuộc tấn công ransomware.

!

RANSOMWARE READINESS

Phát hiện ransomware hiệu quả phải bắt đầu từ các hành vi chuẩn bị: xóa log, credential dumping, tạo service, công cụ remote và kết nối C2.

Điều này cho thấy chống ransomware không chỉ là phát hiện hành vi mã hóa tệp mà SOC cần phát hiện các hành vi tiền ransomware trước khi quá trình mã hóa bắt đầu.

8.2 Khuyến nghị cho doanh nghiệp

- Sử dụng mô hình backup 3-2-1-1-0.
- Có ít nhất một bản sao immutable hoặc offline.
- Tách tài khoản quản trị backup khỏi domain thông thường.
- Hạn chế kết nối từ người dùng tới máy chủ backup.
- Kiểm thử phục hồi định kỳ.
- Giám sát thao tác xóa snapshot và thay đổi retention.
- Phát hiện hành vi vô hiệu hóa EDR.
- Áp dụng danh sách chặn driver dễ bị khai thác.
- Diễn tập ransomware ở cấp kỹ thuật và quản trị.

SECTION 9

Hoạt động APT tại Đông Nam Á đặt doanh nghiệp Việt Nam vào vùng rủi ro

Các chiến dịch gián điệp mạng theo khu vực có thể nhắm vào doanh nghiệp như một mắt xích trong chuỗi cung ứng hoặc hệ sinh thái ngành.

Trong sáu tháng đầu năm 2026, nhiều chiến dịch gián điệp mạng được ghi nhận nhắm vào chính phủ, viễn thông, tài chính, công nghệ và các tổ chức quan trọng tại Đông Nam Á.
Các chiến dịch đáng chú ý đã sử dụng:

- Spear-phishing theo bối cảnh công việc.
- Tài liệu khai thác lỗ hổng.
- Tấn công thiết bị biên.
- Living-off-the-land.
- Dịch vụ đám mây hợp pháp làm Command and Control.

- Công cụ tùy biến để duy trì quyền truy cập dài hạn.

Một số chiến dịch được liên hệ với các nhóm thuộc hệ sinh thái APT41, APT28 và các tác nhân gián điệp khác.

9.1 Nguy cơ đối với doanh nghiệp Việt Nam

Các tổ chức không nhất thiết phải là mục tiêu cuối cùng. Doanh nghiệp có thể bị tấn công để:

- Thu thập thông tin về một ngành hoặc chuỗi cung ứng.
- Xâm nhập đối tác lớn hơn.
- Đánh cắp tài liệu dự án và hợp đồng.
- Theo dõi email lãnh đạo.
- Chuẩn bị hạ tầng cho hoạt động trong tương lai.
- Chiếm tài khoản để phát tán spear-phishing.

9.2 Khuyến nghị cho doanh nghiệp

- Đưa threat intelligence theo khu vực vào hoạt động SOC.
- Theo dõi các TTP thay vì chỉ IOC.
- Thực hiện threat hunting định kỳ.
- Bảo vệ tài khoản lãnh đạo và người dùng có quyền truy cập dữ liệu nhạy cảm.
- Giám sát dịch vụ cloud được sử dụng làm C2.
- Triển khai deception hoặc honeytoken tại vùng dữ liệu quan trọng.
- Thực hiện tabletop exercise cho kịch bản APT.

SECTION 10

Những bài học quan trọng từ hoạt động Threat Monitoring

Giá trị của SOC nằm ở khả năng đặt cảnh báo vào đúng ngữ cảnh vận hành, tài sản và rủi ro.

10.1 Cảnh báo bất thường không đồng nghĩa với tấn công

Nhiều cảnh báo về RDP, SSH, tạo tài khoản, công cụ remote hoặc thay đổi quyền được xác minh là hoạt động nội bộ hợp lệ.

Tuy nhiên, việc xác minh có giá trị vì những hành vi này cũng là kỹ thuật phổ biến của kẻ tấn công.

Doanh nghiệp nên duy trì:

- Danh sách hoạt động bảo trì đã đăng ký.
- Change request.
- Danh sách tài khoản quản trị.
- Danh sách công cụ remote hợp lệ.
- Khung giờ vận hành.
- Baseline hành vi theo hệ thống và người dùng.

10.2 False positive vẫn có thể phản ánh điểm yếu quản trị

Một cảnh báo được đóng là false positive nhưng không có nghĩa là doanh nghiệp không có rủi ro.

Ví dụ:

- Đăng nhập quản trị ngoài giờ có thể là hợp lệ nhưng thiếu kiểm soát.
- Công cụ remote hợp lệ có thể không được quản lý tập trung.
- Tài khoản có mật khẩu không hết hạn có thể phục vụ ứng dụng nhưng vẫn tạo rủi ro.
- Dịch vụ công khai có thể đang được sử dụng nhưng chưa được bảo vệ đầy đủ.
- Tệp nén trong thư mục web có thể phục vụ triển khai nhưng quy trình triển khai chưa được chuẩn hóa.

SOC cần chuyển các phát hiện này thành đề xuất cải thiện kiểm soát, thay vì chỉ đóng cảnh báo.

10.3 Ngữ cảnh quyết định chất lượng phát hiện

Để phát hiện và xử lý mối đe dọa chính xác, SOC không chỉ dựa vào các cảnh báo đơn lẻ mà cần tổng hợp nhiều thông tin liên quan (context), bao gồm:

- Mức độ quan trọng của tài sản hoặc hệ thống bị ảnh hưởng (Asset criticality).
- Đơn vị hoặc cá nhân chịu trách nhiệm quản lý hệ thống.
- Hành vi sử dụng bình thường của người dùng để nhận diện các dấu hiệu bất thường.
- Các thay đổi gần đây trong hệ thống như cập nhật, cấu hình hoặc triển khai mới.
- Thông tin về các mối đe dọa đang được ghi nhận trên toàn cầu (Threat Intelligence).
- Tình trạng lỗ hổng bảo mật của hệ thống.
- Dữ liệu từ thiết bị đầu cuối (Endpoint).
- Dữ liệu từ hệ thống mạng.
- Dữ liệu về danh tính và hoạt động đăng nhập của người dùng.
- Dữ liệu từ môi trường Cloud và các ứng dụng SaaS.

Khi có đầy đủ những thông tin này, SOC sẽ hiểu rõ bối cảnh của từng sự kiện, từ đó xác định chính xác đâu là mối đe dọa thực sự và ưu tiên xử lý các sự cố có mức độ rủi ro cao. Ngược lại, nếu thiếu ngữ cảnh, SOC có thể tạo ra rất nhiều cảnh báo nhưng khó xác định được sự cố nào thực sự cần được xử lý, dẫn đến mất thời gian và giảm hiệu quả vận hành.

SECTION 11

10 khuyến nghị cần ưu tiên cho doanh nghiệp trong nửa cuối năm 2026

Danh sách ưu tiên dưới đây giúp doanh nghiệp chuyển các quan sát từ threat monitoring thành hành động quản trị rủi ro cụ thể.

STT	Ưu tiên	Trọng tâm hành động
1	Quản lý bề mặt tấn công	Kiểm kê tài sản Internet-facing, API, cloud service và giao diện quản trị.
2	Vá lỗi dựa trên rủi ro	Ưu tiên lỗ hổng đang bị khai thác trên tài sản quan trọng.
3	Bảo vệ danh tính	MFA chống phishing, Conditional Access, PAM và giám sát đăng nhập bất thường.
4	Endpoint telemetry	Thu thập process, network, PowerShell, service và scheduled task.
5	SaaS data protection	Giám sát audit log, chia sẻ ra ngoài, tải xuống hàng loạt và OAuth app.
6	Kiểm soát công cụ remote	Allowlist, ticket/change request, giới hạn khung giờ và audit trail.
7	Chống ransomware	Immutable backup, tách quyền, kiểm thử phục hồi và phát hiện tiền ransomware.
8	Chuỗi cung ứng phần mềm	SBOM, quét dependency, bảo vệ CI/CD và luân chuyển secret.
9	Threat hunting	Ưu tiên valid account, C2, defense evasion, credential access và exfiltration.

10	Diễn tập ứng cứu sự cố	Tabletop và diễn tập kỹ thuật cho ransomware, cloud compromise, APT và rò rỉ dữ liệu.

- **Kiểm kê và quản lý bề mặt tấn công:** Xác định toàn bộ tên miền, địa chỉ IP, dịch vụ cloud, VPN, firewall, web application, API và giao diện quản trị kết nối Internet.
- **Vá lỗi dựa trên rủi ro:** Ưu tiên lỗ hổng đang bị khai thác, tài sản Internet-facing, hệ thống quản trị, nền tảng định danh và hệ thống backup.
- **Tăng cường bảo vệ danh tính:** Triển khai MFA chống phishing, Conditional Access, PAM và giám sát rủi ro đăng nhập.
- **Giám sát endpoint chuyên sâu:** Thu thập process creation, network connection, PowerShell, service creation, scheduled task và thay đổi tài khoản.
- **Bảo vệ dữ liệu SaaS:** Thu thập audit log, giám sát chia sẻ ra ngoài, tải xuống hàng loạt và ứng dụng OAuth.
- **Kiểm soát công cụ remote:** Chỉ cho phép công cụ được phê duyệt và giám sát toàn bộ phiên truy cập đặc quyền.
- **Củng cố khả năng chống ransomware:** Tách hệ thống backup, sử dụng immutable backup và kiểm thử phục hồi.
- **Quản lý chuỗi cung ứng phần mềm:** Duy trì SBOM, quét thư viện mã nguồn và bảo vệ pipeline CI/CD.
- **Xây dựng chương trình threat hunting:** Ưu tiên các giả thuyết liên quan đến valid account, C2, defense evasion, credential access và data exfiltration.
- **Diễn tập ứng cứu sự cố:** Thực hiện tabletop exercise và diễn tập kỹ thuật cho các kịch bản:
    - Tài khoản cloud bị chiếm.
    - VPN hoặc firewall bị xâm nhập.
    - Web server bị cài webshell.
    - Ransomware.
    - Rò rỉ dữ liệu.
    - Chuỗi cung ứng phần mềm bị xâm nhập.
    - DDoS.
    - APT duy trì hiện diện dài hạn.

03 hành động cần thực hiện ngay

03 ưu tiên ngắn hạn giúp doanh nghiệp giảm nhanh rủi ro từ bề mặt tấn công, ransomware và danh tính.

Nếu doanh nghiệp chỉ có thể ưu tiên 03 nhiệm vụ trong thời gian ngắn, nên tập trung vào 03 hành động sau:

01 | INTERNET-FACING	02 | RANSOMWARE	03 | IDENTITY & SAAS
Rà soát toàn bộ tài sản Internet-facing.	**Kiểm tra khả năng phục hồi ransomware.**	**Tăng cường giám sát danh tính và SaaS.**
Đóng dịch vụ không cần thiết, vá lỗ hổng và thay đổi thông tin xác thực có nguy cơ bị lộ.	Xác nhận bản sao lưu không thể bị xóa từ tài khoản production và thử nghiệm khôi phục thực tế.	Phát hiện đăng nhập hiếm gặp, brute force, thay đổi MFA, chia sẻ dữ liệu ra ngoài và tải xuống bất thường.

Các sự kiện trong sáu tháng đầu năm 2026 cho thấy doanh nghiệp đang đối mặt với một hệ sinh thái đe dọa có tính liên kết cao.

Một cuộc tấn công có thể bắt đầu từ mật khẩu bị đánh cắp, tiếp tục bằng đăng nhập VPN, quét mạng nội bộ, sử dụng PowerShell, thu thập thông tin xác thực, tạo tài khoản, xóa log và cuối cùng triển khai ransomware hoặc đánh cắp dữ liệu.

Các tín hiệu ban đầu của chuỗi tấn công thường đã xuất hiện trong hệ thống trước khi phát triển thành sự cố nghiêm trọng — giá trị của SOC là liên kết và xử lý sớm các tín hiệu này.

Dữ liệu giám sát thực tế của HSOC cho thấy các tín hiệu ban đầu của chuỗi tấn công thường đã xuất hiện trong hệ thống. Thách thức không chỉ nằm ở việc thu thập cảnh báo, mà ở khả năng liên kết, xác minh và phản ứng trước khi các hành vi riêng lẻ phát triển thành một sự cố nghiêm trọng.

CHUYỂN DỊCH MÔ HÌNH PHÒNG THỦ

Doanh nghiệp cần chuyển từ phòng thủ dựa trên sản phẩm sang vận hành an toàn thông tin liên tục.

Doanh nghiệp cần chuyển từ mô hình phòng thủ dựa trên sản phẩm sang mô hình vận hành an toàn thông tin liên tục, bao gồm:

- Quản lý bề mặt tấn công.
- Bảo vệ danh tính.
- Quản lý lỗ hổng theo rủi ro.
- Giám sát tập trung 24/7.
- Threat intelligence.
- Threat hunting.
- Phản ứng sự cố.
- Khả năng phục hồi đã được kiểm chứng.

Trong bối cảnh các nhóm tấn công khai thác lỗ hổng nhanh hơn và sử dụng công cụ hợp pháp để né tránh phát hiện, tốc độ xác định đúng bản chất sự kiện và phối hợp xử lý sẽ là yếu tố quyết định mức độ thiệt hại của doanh nghiệp.

SECTION 12

Giải pháp phòng thủ toàn diện từ HPT

Để chủ động bảo vệ doanh nghiệp trước các mối đe dọa ngày càng tinh vi, HPT cung cấp các giải pháp và dịch vụ an toàn thông tin chuyên biệt:

- **Dịch vụ Kiểm thử xâm nhập (Penetration Testing):** Giả lập tấn công để phát hiện các điểm yếu trên bề mặt hệ thống của tổ chức trước khi kẻ xấu khai thác.
- **Dịch vụ Giám sát an toàn thông tin 24x7 (SOC):** Theo dõi liên tục, phát hiện và ngăn chặn các hành vi tấn công đáng ngờ trên các máy chủ và máy tính người dùng.
- **Dịch vụ Tư vấn bảo mật:** Xây dựng quy trình sao lưu (backup) theo chuẩn 3-2-1 và diễn tập phục hồi, đảm bảo dữ liệu luôn an toàn và sẵn sàng.
- **Dịch vụ Đánh giá và đào tạo nhận thức người dùng (Email Phishing):** Củng cố "bức tường lửa con người", lớp phòng thủ quan trọng nhất của doanh nghiệp.

Đừng chờ đợi sự cố xảy ra. Hãy liên hệ với HPT ngay hôm nay để được tư vấn và xây dựng một lá chắn bảo vệ vững chắc cho doanh nghiệp của bạn!

III. Câu hỏi thường gặp

1. Những mối đe dọa an ninh mạng nổi bật nhất trong sáu tháng đầu năm 2026 là gì?
Các mối đe dọa nổi bật gồm khai thác VPN và thiết bị biên, đánh cắp danh tính, tấn công ứng dụng web, ransomware, mã độc đánh cắp thông tin, tấn công chuỗi cung ứng và hoạt động APT tại Đông Nam Á.

2. HSOC thường phát hiện những hành vi bất thường nào?
Các hành vi thường gặp gồm brute force, đăng nhập từ vị trí hiếm gặp, kết nối C2, truy vấn DNS đáng ngờ, quét cổng, khai thác ứng dụng web, sử dụng công cụ remote, thay đổi quyền tài khoản và tải xuống dữ liệu bất thường.

3. False positive có còn giá trị đối với doanh nghiệp không?
Có. False positive có thể phản ánh những điểm yếu trong quản trị thay đổi, quản lý tài khoản, kiểm soát công cụ remote hoặc cấu hình hệ thống. Những trường hợp này nên được sử dụng để cải thiện baseline và kiểm soát nội bộ.

4. Doanh nghiệp cần làm gì để chống ransomware?
Doanh nghiệp cần vá lỗ hổng, bảo vệ tài khoản đặc quyền, phân đoạn mạng, triển khai EDR, giám sát các hành vi tiền ransomware và duy trì bản sao lưu immutable hoặc offline đã được kiểm thử khôi phục.

5. Vì sao cần liên kết dữ liệu mạng, endpoint và danh tính?

Một nguồn log riêng lẻ thường chỉ phản ánh một phần của cuộc tấn công. Việc kết hợp network, endpoint, identity, cloud và threat intelligence giúp SOC tái dựng chuỗi hành vi và phân biệt hoạt động hợp lệ với xâm nhập thực tế.

6. Threat monitoring khác gì với giám sát cảnh báo thông thường?
Threat monitoring không chỉ xử lý từng cảnh báo riêng lẻ. Hoạt động này liên kết sự kiện theo người dùng, thiết bị, thời gian, chiến thuật và kỹ thuật tấn công để xác định các chuỗi hành vi có nguy cơ cao.

TÀI LIỆU THAM KHẢO

- Thông tin giám sát từ HSOC.
- Thông tin Threat Intelligence từ HSOC.
- 2026 Cyberthreat Defense Report, CyberEdge Group (do ISC2 tài trợ).
- Coveware Quarterly Ransomware Reports (Q2–Q4/2025).
- CrowdStrike Global Threat Report (H1 2025); Sophos Incident Response 2025; Recorded Future 2025.

Liên hệ

Văn phòng Tổng công ty
Lô E2a-3 Đường D1, Khu Công nghệ cao, Phường Tăng Nhơn Phú, TP. HCM
Tel: +(84 28) 38 266 206 | **Email:** info@hpt.vn
Website: https://hpt.vn

HPT Vietnam Corporation

Trung tâm Dịch vụ Khách hàng
Số 37 Nguyễn Trường Tộ, Phường Xóm Chiếu, TP. HCM
Tel: +(84 28) 38 266 206 | **Hotline:** 18006686

Văn phòng Chi nhánh Hà Nội
Tầng 10, tòa nhà Việt, số 1 Thái Hà, Phường Đống Đa, TP. Hà Nội
Tel: +(84 28) 38 266 206