Trending Threats & Vulnerabilities: Phạm Vi Bao Phủ của Falcon Đối Với Các Kỹ Thuật Tấn Công Liên Quan Đến F5

Solution: Cloud Security Modules (CSPM & CWP) | Endpoint Security | Sensors - Linux OS Platforms | Next-Gen SIEM

Ngày công bố: 16/10/2025

Tóm Tắt

Vào ngày 15 tháng 10 năm 2025, F5, Inc. đã thông báo về một sự cố an ninh được quy cho một kẻ tấn công tinh vi. Để biết thêmthông tin, vui lòng tham khảo tài liệu K000154696: F5 Security Incident (https://my.f5.com/manage/s/article/K000154696). CrowdStrike đã hợp tác với F5 và các tổ chức khác bị nhắm mục tiêu bởi kẻ tấn công này, triển khai các biện pháp chủ động để bảo vệ khách hàng của chúng tôi khỏi các cuộc tấn công tương tự bằng cách tận dụng các chiến thuật, kỹ thuật và quy trình (TTPs) của kẻ tấn công. Sự cố này nhấn mạnh nhu cầu cấp thiết về khả năng quan sát và phát hiện toàn diện trên mọi bề mặt tấn công.

Tôi có bị ảnh hưởng không?

F5 đã vá tất cả các lỗ hổng đã biết (Tham khảo trong tài liệu K000156572: Quarterly Security Notification (October 2025) (https://my.f5.com/manage/s/article/K000156572)) và khách hàng nên cập nhật lên các phiên bản này ngay lập tức. Mặc dù CrowdStrike không có bằng chứng nào về việc các thiết bị F5 bị khai thác trên diện rộng, chúng tôi đặc biệt khuyến nghị nên thực hiện đánh giá các biện pháp kiểm soát an ninh cho các thành phần mạng và hạ tầng thường xuyên bị kẻ tấn công nhắm mục tiêu.

Khách hàng có thể thực hiện những hành động nào?

- Đảm bảo các môi trường nội bộ và bên ngoài, bao gồm các thiết bị mạng ở vùng biên (edge), các máy chủ VMware ESXi và các hệ thống VMware vCenter Server đều được vá lỗi đầy đủ.
- Giới hạn quyền truy cập vào management và control planes, chỉ cho phép các mạng quản trị được chỉ định.
- Cấu hình các sản phẩm của third party để bật ghi log và chuyển tiếp các log đó đến Falcon NG-SIEM.
- Tận dụng lợi ích từ Falcon sensor cho F5 BIG-IP của chúng tôi bằng cách tham gia Chương trình Truy cập Sớm (Early Access Program) và triển khai Falcon sensor lên các thiết bị BIG-IP.

Falcon sensor cho F5 BIG-IP

CrowdStrike đã hợp tác với F5 để phát hành phiên bản Falcon sensor hỗ trợ cho các thiết bị BIG-IP. Falcon Sensor cho Linux đã được cập nhật để hỗ trợ F5 TMOS, vốn được xây dựng trên nền tảng CentOS. Bằng cách chạy trực tiếp trên các thiết bị F5 BIG-IP, Falcon Sensor có thể phát hiện các mối đe dọa bằng cách sử dụng cùng một phạm vi bao phủ có sẵn dùng để bảo vệ các workload Linux khác. CrowdStrike cũng đang tích cực phát triển nội dung phát hiện mới, tập trung đặc biệt vào việc lập mô hình mối đe dọa cho các thiết bị mạng.

Khách hàng của CrowdStrike nên truy cập tài liệu K000157015: Getting Started with Falcon sensor for BIG-IP (https://my.f5.com/manage/s/article/K000157015) để tham gia Chương trình Truy cập Sớm (Early Access Program) nhằm bắt đầu cài đặt các sensor trên thiết bị F5 BIG-IP của mình. Thông tin chi tiết hơn về việc cài đặt và quản lý các Falcon Sensor cho BIG-IP sẽ được cung cấp trong khuôn khổ của chương trình EAP. Vui lòng xem Falcon Sensor cho F5 BIG-IP VE 17.1.3 và 17.5.1.3 (https://supportportal.crowdstrike.com/s/article/Falcon-Sensor-for-F5- BIG-IP-VE-17-1-3-and-17-5-1-3) để biết thêm thông tin.

Phạm vi bao phủ của Nền tảng CrowdStrike Falcon

Để tối đa hóa phạm vi bao phủ cho các TTPs ở mỗi lớp hạ tầng, chúng ta có thể chia nhỏ các cuộc tấn công thành một vài khu vực trọng tâm:

Vùng biên Mạng (Network Edge)

Các điểm truy cập vào mạng (ingress points) và các interface quản lý có kết nối ra ngoài internet là những mục tiêu thường gặp ở giai đoạn Xâm nhập Ban đầu (initial access). Việc duy trì khả năng quan sát đối với các hoạt động đáng ngờ tại vùng biên của mạng sẽ cung cấp cho các đội ngũ SOC một lợi thế sớm. Nền tảng Falcon cung cấp các công cụ để tối đa hóa phạm vi bao phủ trong khu vực này:

- **Falcon NG-SIEM:** Khách hàng nên cấu hình các thiết bị mạng để ghi log tất cả hoạt động có liên quan và chuyển tiếp các log này đến Falcon NG-SIEM. Đối với việc cấu hình thiết bị F5 BIG-IP, hãy tham khảo tài liệu **F5 BIG-IP Data Connector | US-2 (https://falcon.us-2.crowdstrike.com/documentation/page/ob38708b/f5-big-ip-data-connector).** Sau khi bật tính năng thu thập dữ liệu, hãy kích hoạt Rule Templates phù hợp được liệt kê bên dưới.

- **Falcon sensor cho F5 BIG-IP:** Khách hàng hiện tại có thể cài đặt Falcon sensor trực tiếp trên các thiết bị F5 BIG-IP. Điều này giúp tăng cường đáng kể khả năng quan sát từ lớp hệ điều hành, cho phép Falcon giám sát hoạt động ở mức độ sâu hơn so với việc ghi log truyền thống. Các log được thu thập bởi NG-SIEM và khả năng quan sát từ Falcon sensor cho F5 BIG-IP nên được sử dụng như các giải pháp bổ trợ cho nhau.

Hạ tầng Hosting

Kẻ tấn công thường xuyên nhắm mục tiêu vào hạ tầng máy ảo hosting, bao gồm các on-premise hypervisors và các management planes trên public cloud. Việc có được khả năng quan sát vào các môi trường này là cực kỳ quan trọng để đội ngũ phòng thủ có thể truy vết dòng thời gian của các cuộc tấn công trải dài từ hệ điều hành đến các máy chủ vật lý bên dưới. Nền tảng Falcon cung cấp khả năng quan sát này thông qua các phương pháp sau:

- **Falcon Cloud Security:** Khách hàng sử dụng Falcon Cloud Security nên tận dụng các khả năng của nó để phân tích trạng thái bảo mật của cloud, chủ động củng cố hệ thống phòng thủ của mình. Các Dấu hiệu Tấn công Dựa trên Hành vi (Behavioral IOAs) được triển khai để phát hiện hoạt động độc hại trên cả management plane và môi trường runtime.
- **Falcon Next-Gen SIEM (NG-SIEM):** Các hypervisor và các hạ tầng hosting khác nên được cấu hình để tạo và chuyển tiếp log đến các bộ kết nối dữ liệu (data connectors) của NG-SIEM. Các Rule Templates được đề xuất bên dưới là dành cho mục đích này.

Các mục tiêu của Lateral Movement

Mặc dù mỗi cuộc tấn công thường mang tính chất "duy nhất", nhưng hầu hết chúng đều bao gồm việc kẻ tấn công di chuyển qua các mạng khác để thiết lập một chỗ đứng vững chắc hơn và xác định các mục tiêu có giá trị cao. Vấn đề phức tạp này đòi hỏi phải có một giải pháp đa diện, kết hợp các phương pháp bảo mật tốt nhất như phòng thủ theo chiều sâu (defense-in-depth) và quyền hạn tối thiểu (least privilege) với các thành phần sau của nền tảng Falcon:

- **Falcon Insight and Prevent:** Falcon sensor nên được triển khai ở mọi nơi được hỗ trợ và các Chính sách Ngăn chặn (Prevention Policies) nên được cấu hình theo các khuyến nghị tốt nhất. Các Falcon sensor được cấu hình đúng cách sẽ ngăn chặn các cuộc tấn công thông qua sự kết hợp giữa AI/ML và phát hiện dựa trên hành vi.
- **Falcon NG-SIEM:** Khách hàng nên tiến hành lập mô hình mối đe dọa (threat modeling) một cách kỹ lưỡng cho hệ thống mạng của mình để xác định các mục tiêu có hành vi Lateral movement tiềm ẩn. Bất kỳ hệ thống hoặc ứng dụng nào tạo ra dữ liệu (telemetry) có liên quan đều nên được cấu hình để tích hợp với NG-SIEM. Dữ liệu này có thể đóng vai trò là nguồn dữ liệu (telemetry) chính hoặc làm phong phú hơn cho các dữ liệu từ Falcon Sensor hiện có.

Tập trung vào kẻ tấn công

Mỗi kẻ tấn công đều sử dụng các chiến lược riêng biệt và Đội Counter Adversary Operations của Falcon tiếp tục dẫn đầu trong việc thấu hiểu và ứng phó với các hành vi cụ thể của chúng. Mọi sản phẩm trong nền tảng Falcon đều được tối ưu hóa để ngăn chặn các sự cố xâm nhập, từ threat Intelligence đến các khả năng phát hiện và ngăn chặn tích hợp.

- **Phạm vi Bao phủ Webshell trên Linux:** CrowdStrike Falcon cung cấp khả năng phát hiện toàn diện đối với các webshell được sử dụng cho việc xâm nhập ban đầu và duy trì truy cập. Khả năng quan sát script on-write của Falcon giúp xác định hành vi triển khai webshell ngay khi các script độc hại được ghi vào hệ thống file của các máy bị xâm nhập. Cách tiếp cận nhận biết theo ngữ cảnh này giúp phát hiện cả các webshell đã biết và các biến thể mới, cung cấp khả năng quan sát hoàn chỉnh về các hành động của kẻ tấn công. Khả năng quan sát PHP nâng cao giúp củng cố việc phát hiện các webshell dựa trên PHP, vốn thực thi động code do kẻ tấn công cung cấp bằng các hàm như eval, assert hoặc create_function, đây đều là những kỹ thuật phổ biến trong việc triển khai webshell. Kết hợp với các Dấu hiệu tấn công dựa trên hành vi (Behavioral IOAs) giúp phát hiện các hành vi saukhai thác (ví dụ: tạo ra các tiến trình con đáng ngờ từ các dịch vụ web, thực thi các lệnh hệ thống và thiết lập các reverse shell), Falcon mang lại khả năng phát hiện và ngăn chặn theo thời gian thực đối với các kỹ thuật xâm nhập dựa trên webshell.
- **BRICKSTORM:** Như đã được đề cập chi tiết trong tài liệu **CSA-250969 |** US-2 (https://falcon.us- 2.crowdstrike.com/intelligence-v2/reports/csa-250969), BRICKSTORM là một backdoor đa nền tảng tinh vi được phát triển bằng ngôn ngữ Go. Nó thiết lập quyền truy cập lâu dài cho các kẻ tấn công và bao gồm các khả năng proxy SOCKS, biến các endpoint bị xâm nhập thành các điểm bàn đạp chiến lược (pivot points). Điều này cho phép kẻ tấn công định tuyến lưu lượng độc hại qua các hệ thống bị nhiễm trong khi vẫn che giấu hạ tầng C&C của chúng. Các kẻ tấn công đã bị quan sát thấy đang triển khai backdoor này trên các thiết bị mạng và những hạ tầng thiếu các công cụ phát hiện và phản ứng endpoint điển hình. Khách hàng nên đảm bảo rằng các dữ liệu (telemetry) từ các mục tiêu tiềm ẩn này được thu thập bằng Falcon NG-SIEM và các Rule Templates có liên quan đã được bật.
- **Junction & GuestConduit:** Các implant mới dựa trên Golang, được ghi nhận trong tài liệu **CSA-251079** | US-2 (https://falcon.us-2.crowdstrike.com/intelligence- v2/reports/csa-251079), chúng chạy trên các máy chủ ESXi và các guest OS. Các implant này tạo ra các đường giao tiếp chủ động xuyên qua các lớp hạ tầng bị cô lập. Khách hàng nên tuân thủ các khuyến nghị bảo mật của VMware và đảm bảo các Falcon sensor được cài đặt trên các guest OS.

Phụ lục: Các Khuyến nghị về NG-SIEM Rule Template

Khách hàng muốn tận dụng các rule template dưới đây được khuyến khích tham khảo các tài liệu tích hợp dữ liệu tương ứng với từng nhà cung cấp và sản phẩm. Các khuyến nghị này được dựa trên một phạm vi rộng lớn các thiết bị mạng và các kỹ thuật tấn công của kẻ thù được quan sát thấy xung quanh chúng, chứ không dựa trên bất kỳ sự cố cụ thể nào.

- **Okta** US-2 (https://falcon.us-2.crowdstrike.com/documentation/page/cc573d83/okta-identity-management)
- **F5 BIG-IP** US-2 (https://falcon.us-2.crowdstrike.com/documentation/page/ob38708b/f5-big-ip-data-connector)
- **VMware ESXi** US-2 (https://falcon.us-2.crowdstrike.com/documentation/page/x38607f0/vmware-esxi)
- **VMware vCenter** US-2 (https://falcon.us-2.crowdstrike.com/documentation/page/ODCPRn7E/vmware-vcenter)
- **AWS CloudTrail** US-2 (https://falcon.us-2.crowdstrike.com/documentation/page/fd3bed22/aws-cloudtrail)
- **Microsoft Entra ID** US-2 (https://falcon.us-2.crowdstrike.com/documentation/page/zd4ca92c/data-connector-built-for-microsoft-entra-id)
- **Cisco Secure Firewall ASA** US-2 (https://falcon.us-2.crowdstrike.com/documentation/page/eac0ef68/cisco-secure-firewall-asa)
- **Fortinet FortiGate** US-2 (https://falcon.us-2.crowdstrike.com/documentation/page/e001559f/fortinet-fortigate)

Enable các phát hiện dựa trên địa chỉ IP IOC:

- Generic - Network - IP Address IOC Match

Enable các rule liên quan đến F5:

- F5 - BIG-IP - User Created with Root Role
- F5 - BIG-IP - SSH Login from Public IP Address by Root User
- F5 - BIG-IP - Suspicious Commands Executed by Admin User
- F5 - BIG-IP - New User Created with Admin Role
- F5 - BIG-IP - Bash Executed via Management API from Public IP
- F5 - BIG-IP - Syslog Configuration Disabled
- F5 - BIG-IP - Bash Session Established via TMSH
- F5 - BIG-IP - SSH Login from Public IP Address
- F5 - BIG-IP - New User Created with Root Role
- F5 - BIG-IP - Break Glass Account Usage

Enable các rule liên quan đến VMware:

- VMware - vCenter - VM Created and Accessed Within Short Timeframe
- VMware - vCenter - Excessive UI Searches in Short Period
- VMware - vCenter - WebUI Access from Loopback Address
- VMware - ESXi - Unusual File Extension in VMFS Volumes
- VMware - ESXi - Executable Permissions Applied to Files in High-Risk Directory Locations
- VMware - ESXi - Suspicious VM File Upload via SFTP with Naming Mismatch
- VMware - ESXi - Rogue VM Creation
- VMware - ESXi - vpxuser Service Account Failed Login
- VMware - ESXi - User vpxuser Login via SSH
- VMware - ESXi - Unusual vpxuser Service Account Logon Source
- VMware - ESXi - Shell Login via SSH
- VMware - ESXi - Failed Shell Login via SSH
- VMware - ESXi - New IP for SSH Login Detected
- VMware - ESXi - Potential Unauthorized VMFS Access via SFTP

- VMware - ESXi - SFTP Server Enabled
- VMware - ESXi - SSH Access Enabled
- VMware - ESXi - Virtual Machine Created with Recently Uploaded ISO
- VMware - vCenter - Potential JSP Web Shell

Để biết thêm thông tin về thu thập log VMware, hãy xem CrowdStrike blog: https://www.crowdstrike.com/en-us/blog/falcon-next-gen-siem-protects-against-vmware-vcenter-attacks/ (https://www.crowdstrike.com/en-us/blog/falcon-next-gen-siem-protects-against-vmware-vcenter-attacks/)

Enable các rule bổ sung liên quan đến mối đe dọa này:

- Cisco - ASA - Potential Successful Password Spray Attack
- CrowdStrike - Identity - Short Lived Active Directory Account
- Fortinet - NGFW - Potential Successful Password Spray Attack
- Microsoft - Entra ID - Application/Service Principal Credentials Updated by Service Principal
- Microsoft - Entra ID - Application/Service Principal Credentials Updated by User
- Microsoft - Entra ID - Cross-tenant Access Settings Organization Modified
- Microsoft - Entra ID - Entra Connect Account Anomalous Behaviour
- Microsoft - Entra ID - Global Administrator Role Assigned
- Microsoft - Entra ID - New MFA Device Operating System Observed
- Microsoft - Entra ID - Potential Successful Password Spray Attack
- Microsoft - Entra ID - Privileged Role Assigned to User Account in PIM as Eligible Assignment
- Microsoft - Entra ID - Service Principal Granted Full Access to Exchange Web Services
- Microsoft - Entra ID - Short Lived Account
- Microsoft - M365 - Suspicious Graph API Search for Sensitive Mail
- Okta - SSO - New Device Enrolled for User Account
- Okta - SSO - Potential Successful Password Spray Attack
- Okta - SSO - Short Lived Account

Enable các rule public cloud có liên quan:

- AWS - CloudTrail - Potential Successful Password Spray Attack
- AWS - CloudTrail - AWS EC2 Startup Shell Script Change
- AWS - CloudTrail - EC2 Security Group Opened To the World
- AWS - CloudTrail - EC2 Traffic Mirroring Detected
- AWS - CloudTrail - EC2 Network Access Control List Deleted
- AWS - CloudTrail - EC2 Instance Created with Permissive Security Group Rule
- AWS - CloudTrail - EC2 Instance Created or Modified with Instance Metadata Service Version 1 (IMDSv1)
- AWS - CloudTrail - EC2 Snapshot Attributes Change Attempted
- AWS - CloudTrail - EC2 Instance Export to S3 Bucket Attempted
- AWS - CloudTrail - EC2 Network ACL Entry Created or Modified To Allow Ingress on All or High Range of Open Ports
- AWS - CloudTrail - EC2 Detached Volume Attached to Another Instance
- AWS - CloudTrail - EC2 Instance Profile Association Modified
- AWS - CloudTrail - Multiple EC2 Instances Stopped from External IP Address
- AWS - CloudTrail - EC2 Security Group Anomaly Detection for Sensitive Port Access
- AWS - CloudTrail - EC2 Key Pair Creation Followed by Suspicious Instance Launch
- AWS - CloudTrail - Multiple EC2 Instances Launched from an EC2 Instance

- AWS - CloudTrail - EC2 Instance Associated with Admin IAM Role
- AWS - CloudTrail - Suspicious EC2 Instance Launch Pattern
- AWS - CloudTrail - Multiple EC2 Key Pairs Created
- AWS - CloudTrail - Admin Credential Fetch Attempts from Multiple EC2 Instances
- AWS - CloudTrail - Anomalous EC2 userData Attribute Retrieval
- AWS - CloudTrail - Failed EC2 userData Attribute Retrieval
- AWS - CloudTrail - Suspicious Command Execution via SSM Session on Managed Instance
- AWS - CloudTrail - SSH Public Key Uploaded to EC2 Instance
- Microsoft - Azure - Virtual Machine Deleted by User
- Microsoft - Azure - Custom Script Extension Added to a Virtual Machine
- Microsoft - Azure - Virtual Machine Run Command Executed by Service Principal
- Microsoft - Azure - Virtual Machine Run Command Executed by User
- Microsoft - Azure - Virtual Machine Serial Console Initiated
- Microsoft - Azure - Risky User Observed Creating Virtual Machines

Tài liệu bổ sung

- Falcon Sensor for F5 BIG-IP VE 17.1.3 and 17.5.1.3 (https://supportportal.crowdstrike.com/s/article/Falcon-Sensor-for- F5-BIG-IP-VE-17-1-3-and-17-5-1-3)
- **CSA-250969** US-2 (https://falcon.us- 2.crowdstrike.com/intelligence-v2/reports/csa-250969)
- **CSA-251079** US-2 (https://falcon.us- 2.crowdstrike.com/intelligence-v2/reports/csa-251079)
- F5 K000156881: Install Falcon sensor for BIG-IP on the BIG-IP system (https://my.f5.com/manage/s/article/K000156881)
- F5 K000157015: Getting Started with Falcon sensor for BIG-IP (https://my.f5.com/manage/s/article/K000157015)
- F5 K000157014: F5 Support for Falcon for BIG-IP (https://my.f5.com/manage/s/article/K000157014)
- F5 October 2025 Quarterly Security Notification (https://my.f5.com/manage/s/article/K000156572)