Danh sách kiểm tra Worry-Free Business Security Services cho Mã độc tống tiền REVIL

Mã độc tống tiền tên Revil (được phát hiện bởi Trend Micro có mã Ransom.Win32.SODINOKIBI.AUWUJDFJ) đã được xem xét trên diện rộng.

Worry-Free Business Security có các tính năng chủ động để bảo vệ mạng khỏi cuộc tấn công của mã độc tống tiền.

Đối với các biện pháp chủ động, tính năng Giám sát hành vi sẽ phát hiện và tiêu diệt các hành vi giống mã độc tống tiền

Khuyến nghị đề phòng:

1. Đảm bảo các máy có cài WFBS-SVC và đã được nâng cấp phiên bản và mẫu.

2. Thực hiện theo Cấu hình thực tiễn tốt nhất để ngăn chặn mã tống tiền trong Worry-Free Business Security Services.

Tham khảo: https://success.trendmicro.com/solution/1112168-best-practice-configuration-for-ransomware-prevention-in-worry-free-business-security-services-wfbs

3. Thay đổi cài đặt quét Thời gian thực và Lịch quét từ ActiveAction thành Customized Actions.
   - Nhấp chọn Manual Groups > Configure Policy
   - Scan Settings > bên dưới Real-Time Scan Scheduled Scan, chọn Configure Settings
   - Nhấp chọn tab Actions, dưới Virus/Malware, đổi từ Active Action thành Customized Action.
   - Đảm bảo rằng hành động được chỉ định cho “Probable Malware” được đặt thành “Quarantine”.
   - Nên áp dụng các cài đặt tương tự trên the Manual and Scheduled Scan.

4. Cung cấp CAS để bảo vệ Exchange Online, SharePoint, and OneDrive bằng phương pháp tốt nhất. Tham khảo: Tải xuống file PDF tại đây.

5. Phương pháp tốt nhất cho Network

- Sao lưu dữ liệu thường xuyên, giữ bản sao lưu ngoại tuyến và xác minh quá trình sao lưu được giữ nguyên vẹn. Thường xuyên sao lưu dữ liệu quan trọng để giảm thiểu tối đa nguy cơ tổn thất. Lưu dữ liệu quan trọng ở vị trí an ninh là phương giúp cho tổ chức nhanh chóng hồi phục. Thực hành quy tắc 3-2-1: tạo 3 bản sao ở 2 phương tiện khác nhau với 1 bản sao được lưu trữ bên ngoài: http://blog.trendmicro.com/trendlabs-security-intelligence/world-backup-day-the-3-2-1-rule/?_ga=2.125509321.275958253.1515983682-1070363041.1510016695
- Dữ liệu nhạy cảm không được nằm trên cùng một máy chủ và phân đoạn mạng như trong môi trường thư điện tử.
- Sử dụng xác thực hai yếu tố và mật khẩu mạnh
- Chỉ duy trì cập nhật PowerShell mới nhất và gỡ cài đặt các phiên bản cũ. Tắt một số điểm cuối không cần thiết.

Tham khảo: https://activedirectorypro.com/disable-powershell-with-group-policy/

- Tuân thủ Nguyên tắc đặc quyền tối thiểu, đảm bảo rằng người dùng có mức truy cập tối thiểu để hoàn thành nhiệm vụ. Giới hạn quyền Xác thực quản trị đối với các quản trị viên được chỉ định.
- Triển khai kế hoạch hồi phục, để duy trì và giữ lại nhiều bản sao nhất của dữ liệu nhạy cảm hoặc độc quyền, và máy chủ ở một vị trí riêng biệt, an ninh.

6. Phương pháp gửi email tốt nhất

- Triển khai xác thực, báo cáo và tính tuân thủ thư dựa trên tên miền (DMARC), một hệ thống xác thực giúp giảm thiệu thư rác bằng cách phát hiện email spam sử dụng bảng ghi Hệ thống tên miền(DNS) và chữ kí điện tử.
- Đánh dấu các email từ bên ngoài bằng biểu ngữ cho biết nó đến từ một nguồn bên ngoài. Điều này sẽ hỗ trợ người dùng phát hiện được email giả tạo.
- Triển khai các bộ lọc tại cổng email để lọc các email spam tống tiền, chẳng hạn như nhận biết các dòng có chủ đề độc hại, chặn các địa chỉ IP đáng ngờ trên tường lửa.

Biên dịch bởi Thanh Hiền – Help.pacisoft.com