BÁO CÁO

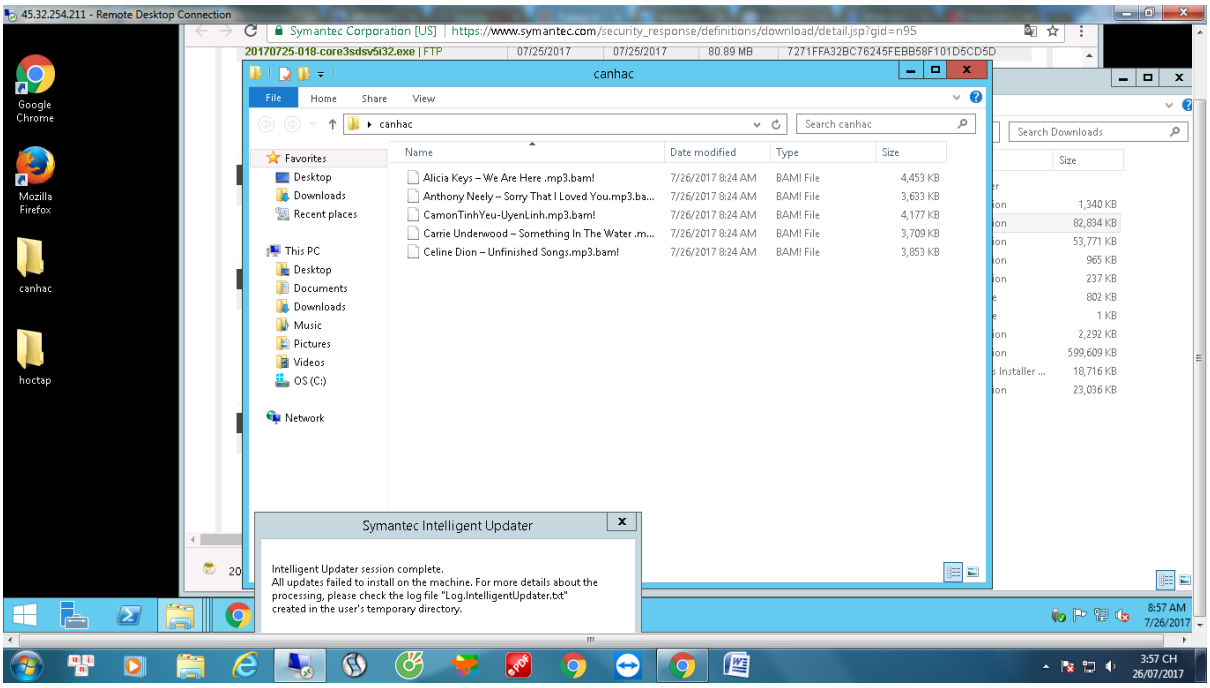
RANSOMWARE:XỬLÝ VÀ PHÒNG CHỐNG

Tên đội: **Drill_TTTTQuangNinh**

Phase 1:

Sau khi mở các file đính kèm, dữ liệu tại các thư mục Desktop, Downloads,… đã bị thay đổi:

Tất cả các file đều bị mã hóa và đổi đuôi thành .bam!



Dự đoán con đường mã độc lây nhiễm vào máy tính:

Thông qua việc mở file doc và kích hoạt Macro

Virut kết nối tới

http://118.70.80.143 (file 1)

http://118.70.80.143:4448 (file 2)

Phase 2:

Cô lập hiện trường và phân tích, lấy mẫu.

Cô lập hiện trường:

Chỉ mở Port 3389 và đóng tất cả các Port khác

Phân tích và lấy mẫu: lấy về file thực thi của ransomware.

Qua file "Diễn tập ANM – 1.doc":

http://118.70.80.143/ransomware.exe

Qua file "Diễn tập ANM – 2.doc":

http://118.70.80.143:4448/ransomware_tb.exe

Phase 3:

Phân tích và xử lý các thành phần độc hại.

Phân tích hành vi file ransomware:

Các thư mục bị mã hóa: Các thư mục Downloads, Desptops và Documents.

Các hành vi khác của mã độc: Chỉnh sủa nội dung trong Registry

Tạo file ransomware trong thư mục C:/Windows/Temp/ransomware.exe

Xử lý các thành phần độc hại: Xóa Registry này đi

Xóa File ransomware trong thư mục C:/Windows/Temp/ransomware.exe

Phase 4:

Điều tra nguồn tấn công và khôi phục dữ liệu bị mã hóa

Các thông tin về nguồn tấn công gồm:

IP server chứa mã độc: 118.70.80.143

Các bước khôi phục dữ liệu:

Xóa registry tại địa chỉ HKEY_CURRENT_USER/Software/whitehatdrill

Xóa File ransomware trong thư mục C:/Windows/Temp/ransomware.exe

Phase 5:

Phòng chống Ransomware bằng phần mềm Anti-virus

Thử nghiệm các file đính kèm khi đã cài đặt Bkav Endpoint

Các biện pháp đề xuất để phòng chống tấn công:

Cái đặt Antivirus Software như BKAV, BitDefender

Up file lên total virut để kiểm tra