# APT28 Targets Hospitality Sector, Presents Threat to Travelers

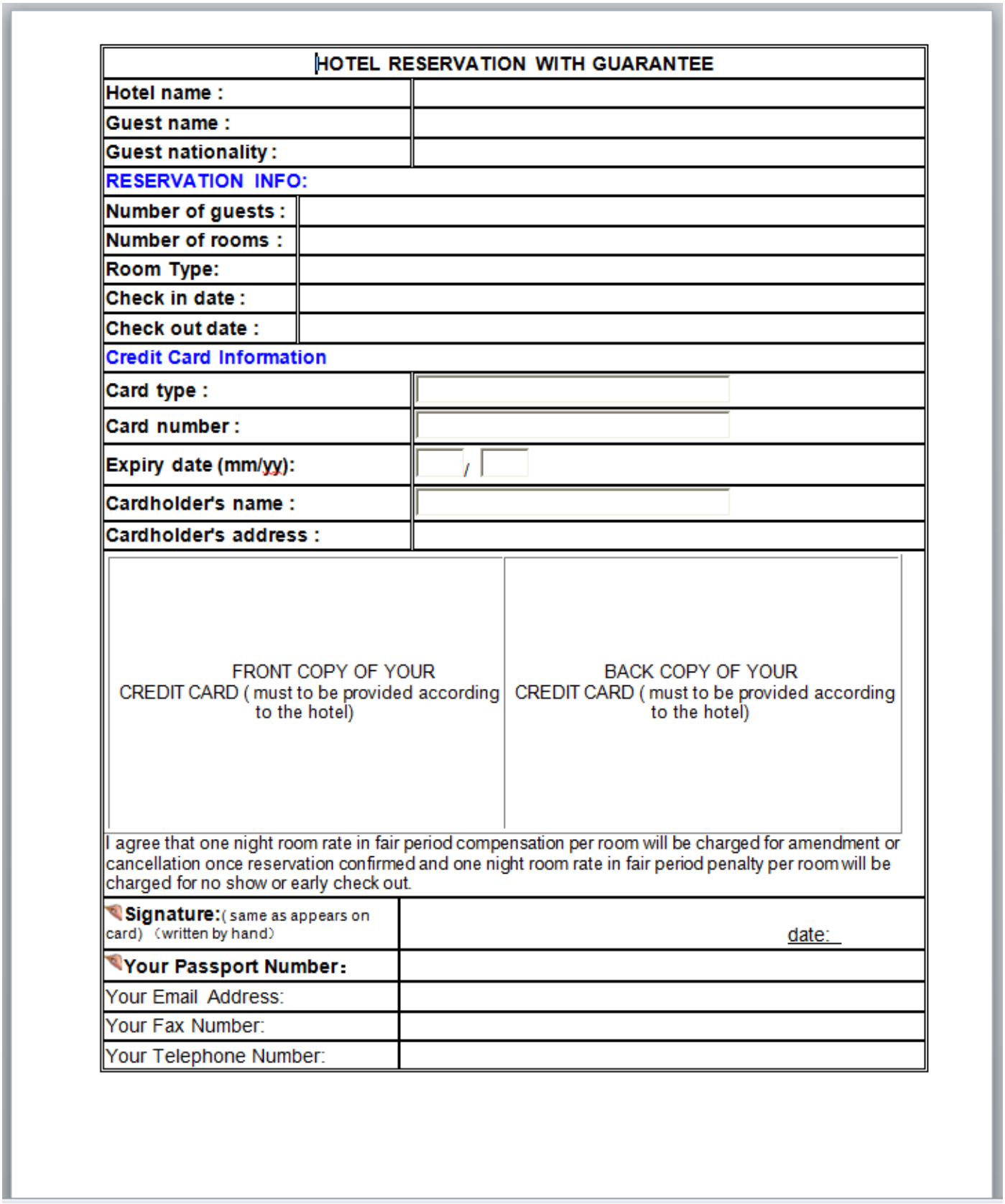
August 11, 2017 | by Lindsay Smith, Ben Read | Threat Research

FireEye has moderate confidence that a campaign targeting the hospitality sector is attributed to Russian actor APT28. We believe this activity, which dates back to at least July 2017, was intended to target travelers to hotels throughout Europe and the Middle East. The actor has used several notable techniques in these incidents such as sniffing passwords from Wi-Fi traffic, poisoning the NetBIOS Name Service, and spreading laterally via the EternalBlue exploit.

## APT28 Uses Malicious Document to Target Hospitality Industry

FireEye has uncovered a malicious document sent in spear phishing emails to multiple companies in the hospitality industry, including hotels in at least seven European countries and one Middle Eastern country in early July. Successful execution of the macro within the malicious document results in the installation of APT28's signature GAMEFISH malware.

The malicious document – Hotel_Reservation_Form.doc (MD5: 9b10685b774a783eabfecdb6119a8aa3), as seen in Figure 1 – contains a macro that base64 decodes a dropper that then deploys APT28's signature GAMEFISH malware (MD5: 1421419d1be31f1f9ea60e8ed87277db), which uses mvband.net and mvtband.net as command and control (C2) domains.



HOTEL RESERVATION WITH GUARANTEE

| | |
|---|---|
| Hotel name : | |
| Guest name : | |
| Guest nationality : | |
| RESERVATION INFO: | |
| Number of guests : | |
| Number of rooms : | |
| Room Type: | |
| Check in date : | |
| Check out date : | |
| Credit Card Information | |
| Card type : | |
| Card number : | |
| Expiry date (mm/yy): | / |
| Cardholder's name : | |
| Cardholder's address : | |

| | |
|---|---|
| FRONT COPY OF YOUR CREDIT CARD ( must to be provided according to the hotel) | BACK COPY OF YOUR CREDIT CARD ( must to be provided according to the hotel) |

I agree that one night room rate in fair period compensation per room will be charged for amendment or cancellation once reservation confirmed and one night room rate in fair period penalty per room will be charged for no show or early check out.

| | |
|---|---|
| Signature:( same as appears on card) （written by hand） | date: |
| Your Passport Number: | |
| Your Email Address: | |
| Your Fax Number: | |
| Your Telephone Number: | |

Figure 1: Hotel_Reservation_Form.doc (MD5: 9b10685b774a783eabfecdb6119a8aa3)

## APT28 Uses Novel Techniques to Move Laterally and Potentially Target Travelers

APT28 is using novel techniques involving the EternalBlue exploit and the open source tool Responder to spread laterally through networks and likely target travelers. Once inside the network of a hospitality company, APT28 sought out machines that controlled both guest and internal Wi-Fi networks. No guest credentials were observed being stolen at the compromised hotels; however, in a separate incident that occurred in Fall 2016, APT28 gained initial access to a victim's network via credentials likely stolen from a hotel Wi-Fi network.

Upon gaining access to the machines connected to corporate and guest Wi-Fi networks, APT28 deployed Responder. Responder facilitates NetBIOS Name Service (NBT-NS) poisoning. This technique listens for NBT-NS (UDP/137) broadcasts from victim computers attempting to connect to network resources. Once received, Responder masquerades as the sought-out resource and causes the victim computer to send the username and hashed password to the attacker-controlled machine. APT28 used this technique to steal usernames and hashed passwords that allowed escalation of privileges in the victim network.

To spread through the hospitality company's network, APT28 used a version of the EternalBlue SMB exploit. This was combined with the heavy use of py2exe to compile Python scripts. This is the first time we have seen APT28 incorporate this exploit into their intrusions.

In the 2016 incident, the victim was compromised after connecting to a hotel Wi-Fi network. Twelve hours after the victim initially connected to the publicly available Wi-Fi network, APT28 logged into the machine with stolen credentials. These 12 hours could have been used to crack a hashed password offline. After successfully accessing the machine, the attacker deployed tools on the machine, spread laterally through the victim's network, and accessed the victim's OWA account. The login originated from a computer on the same subnet, indicating that the attacker machine was physically close to the victim and on the same Wi-Fi network.

We cannot confirm how the initial credentials were stolen in the 2016 incident; however, later in the intrusion, Responder was deployed. Since this tool allows an attacker to sniff passwords from network traffic, it could have been used on the hotel Wi-Fi network to obtain a user's credentials.

## Long-Standing Threats to Travelers

Cyber espionage activity against the hospitality industry is typically focused on collecting information on or from hotel guests of interest rather than on the hotel industry itself, though actors may also collect information on the hotel as a means of facilitating operations. Business and government personnel who are traveling, especially in a foreign country, often rely on systems to conduct business other than those at their home office, and may be unfamiliar with threats posed while abroad.

APT28 isn't the only group targeting travelers. South Korea-nexus Fallout Team (aka Darkhotel) has used spoofed software updates on infected Wi-Fi networks in Asian hotels , and Duqu 2.0 malware has been found on the networks of European hotels used by participants in the Iranian nuclear negotiations. Additionally, open sources have reported for several years that in Russia and China, high-profile hotel guests may expect their hotel rooms to be accessed and their laptops and other electronic devices accessed.

## Outlook and Implications

These incidents show a novel infection vector being used by APT28. The group is leveraging less secure hotel Wi-Fi networks to steal credentials and a NetBIOS Name Service poisoning utility to escalate privileges. APT28's already wide-ranging capabilities and tactics are continuing to grow and refine as the group expands its infection vectors.

Travelers must be aware of the threats posed when traveling – especially to foreign countries – and take extra precautions to secure their systems and data. Publicly accessible Wi-Fi networks present a significant threat and should be avoided whenever possible.

Additional technical information and details are available to FireEye iSIGHT Intelligence customers through our portal.

This entry was posted on Fri Aug 11 09:00:00 EDT 2017 and filed under APT, Ben Read, Blog, Latest Blog Posts, Lindsay Smith, Spear Phishing, Targeted Attacks, and Threat Research.

Communication Preferences

**Technical Support**

Incident?
Report Security Issue
Contact Support
Customer Portal
Communities
Documentation Portal

**Cyber Threat Map**



Privacy & Cookies Policy | Privacy Shield | Legal Documentation