HOW FIN7 ATTACKED AND STOLE DATA

Sophisticated Social Engineering: Phishing & Calling

FIN7 typically initiated its cyberattacks by delivering a "phishing" email to a company employee. Each email included an attached file, often an innocuous-appearing Microsoft Word document, with embedded malware. The text within the email simulated a legitimate business-related message in order to lead the recipient employee to open the attachment and unwittingly activate the malware that would infect the computer. For example, when targeting a hotel chain, the sender of the phishing email might claim to be interested in making a reservation with details enclosed in the attachment. When targeting a restaurant, the phishing email might refer to placing a large catering order or voice a complaint about prior service or food quality, further described in an attachment. Examples of phishing emails deployed by FIN7 are below.

In many cases, FIN7 would accompany the phishing emails with a telephone call to the victim company employee about the same topic, which was intended to legitimize the phishing email. The caller often directed the employee to the recently sent phishing email to further entice the employee to open the attached file and activate the malware.

Network Intrusion: Control & Data Exfiltration

Once infected, the compromised victim computer connected to one of FIN7's command and control servers located throughout the world. Through a specially designed control panel, FIN7 could download a wide array of additional malware to the victim computer, remotely send commands and receive data, and move laterally through the company's network. Among other tools, FIN7 incorporated and adapted the notorious Carbanak malware, which was used by other cybercriminals in a massive transnational attack on the banking industry. FIN7's malware allowed its members to conduct surveillance on company employees, including taking screen shots and even video recordings of desktop activity, enabling them to secretly steal credentials and other network information. FIN7 then used its unauthorized access to the victim's computer system to locate and extract various information and property of value, such as financial information and caches of customer payment card data.

FIN7 most commonly focused on fast-food and casual dining restaurants, hotels, casinos, and businesses with a high frequency of point-of-sale transactions, including businesses with dozens of locations operating in Western Washington. With these and other victims, FIN7

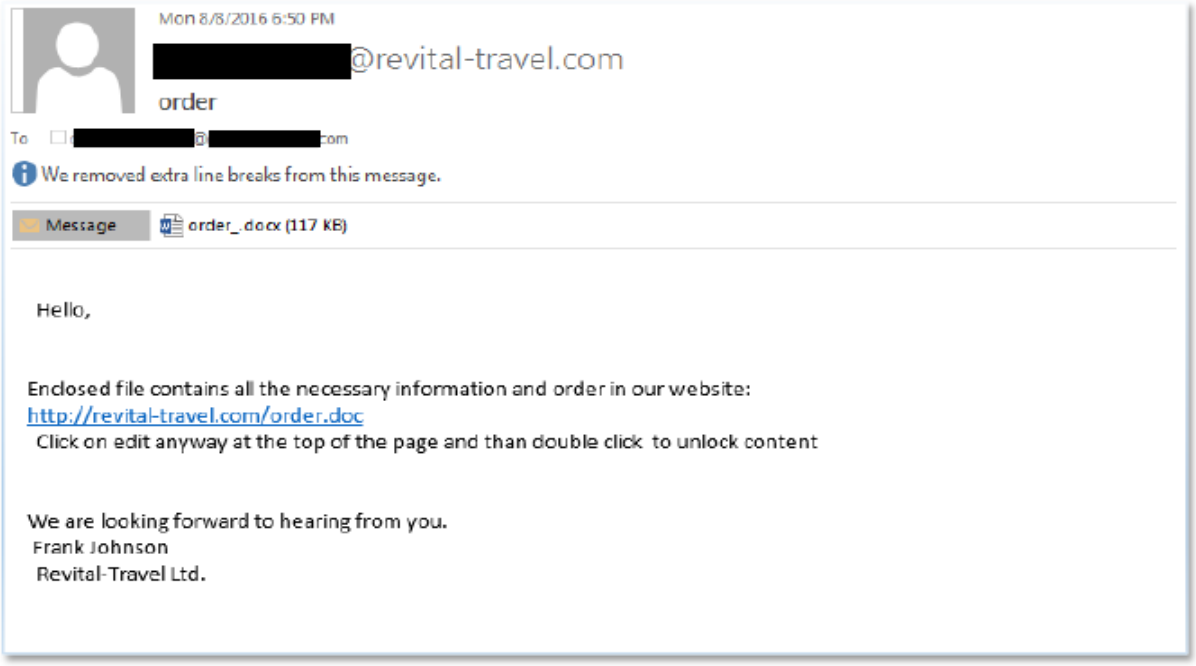
sought to steal credit, debit, and in some cases gift card data, used during legitimate customer purchases.

Selling Stolen Cards

Since 2015, FIN7 successfully stole data for more than 15 million payment cards, many of which have been offered for sale through online underground marketplaces for stolen data. The purchasers could then use the stolen card numbers to make unauthorized charges on accounts belonging to unsuspecting cardholders. Investigators have observed typical retail purchases as well as the purchase of gift cards.

Who is FIN7?

FIN7 is one of the most sophisticated and aggressive malware schemes in recent times, consisting of dozens of talented hackers located overseas. FIN7 uses an arsenal of constantly evolving malware tools and hacking techniques, and controls infected computers through a complex web of servers located throughout the world. The masterminds behind the criminal enterprise created a fake computer security business called Combi Security which they used to recruit new members and to add a thin veil of legitimacy to the hacking scheme. However, there was nothing legitimate about the scores of attacks FIN7 launched against over 100 unsuspecting victims.



Mon 8/8/2016 6:50 PM

[redacted]@revital-travel.com

order

To [redacted]com

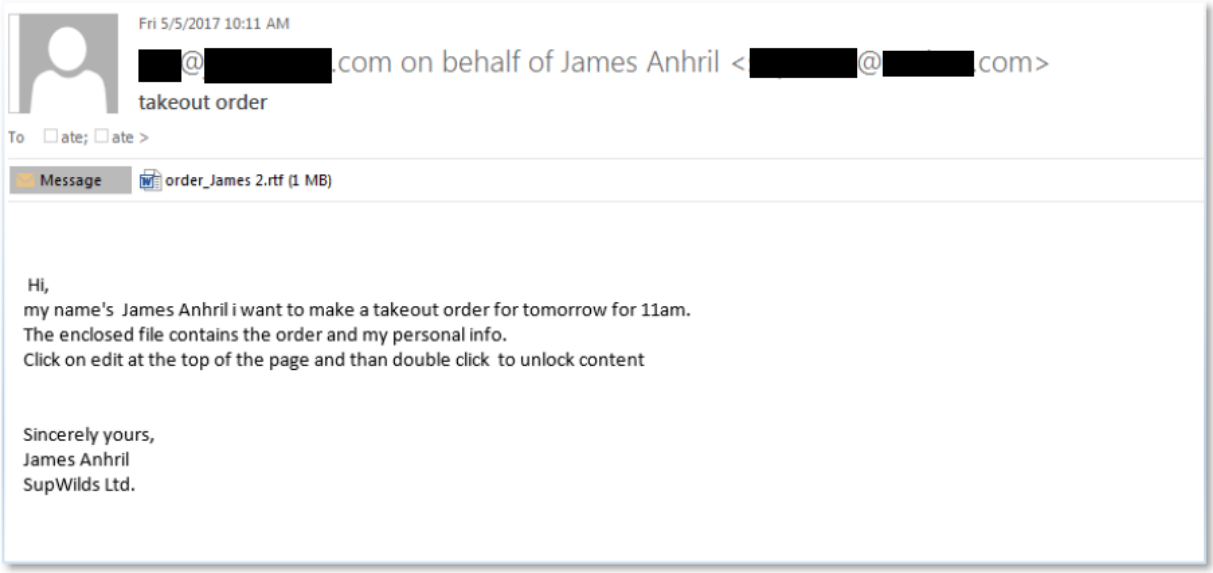
We removed extra line breaks from this message.

Message order_.docx (117 KB)

Hello,

Enclosed file contains all the necessary information and order in our website:
http://revital-travel.com/order.doc
Click on edit anyway at the top of the page and than double click to unlock content

We are looking forward to hearing from you.
Frank Johnson
Revital-Travel Ltd.



Fri 5/5/2017 10:11 AM

[redacted].com on behalf of James Anhril <[redacted]@[redacted].com>

takeout order

To [redacted]ate; [redacted]ate >

Message order_James 2.rtf (1 MB)

Hi,
my name's James Anhril i want to make a takeout order for tomorrow for 11am.
The enclosed file contains the order and my personal info.
Click on edit at the top of the page and than double click to unlock content

Sincerely yours,
James Anhril
SupWilds Ltd.