



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

HC3 Threat Intelligence Briefing FIN7

OVERALL CLASSIFICATION IS
UNCLASSIFIED

TLP:GREEN

8/9/2018

Agenda

- ▶ Intro
- ▶ Overview
- ▶ Relevance
- ▶ FIN7 Background
- ▶ Recent Indictments
 - Individual Roles
- ▶ Operations
- ▶ Impacts
- ▶ Campaigns
 - BATELEUR Malware
- ▶ Protection Recommendations
- ▶ Conclusions



Slides Key:



Non-Technical: managerial, strategic and high-level (general audience)



Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)



Overview

Threat Actor: “FIN7”

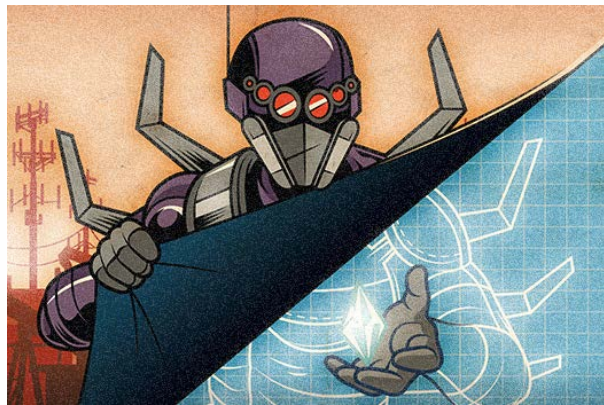
ACTIVE SINCE: 2013

ALIASES: Carbanak / Cobalt Group / Carbon Spider

TARGETS: Restaurants, Hospitality, Casinos and Gaming, Energy, Finance, High-tech, Software, Travel, Education, Construction, Retail, Telecommunications, Government, Business services

OPERATIONS: *Highly Targeted*

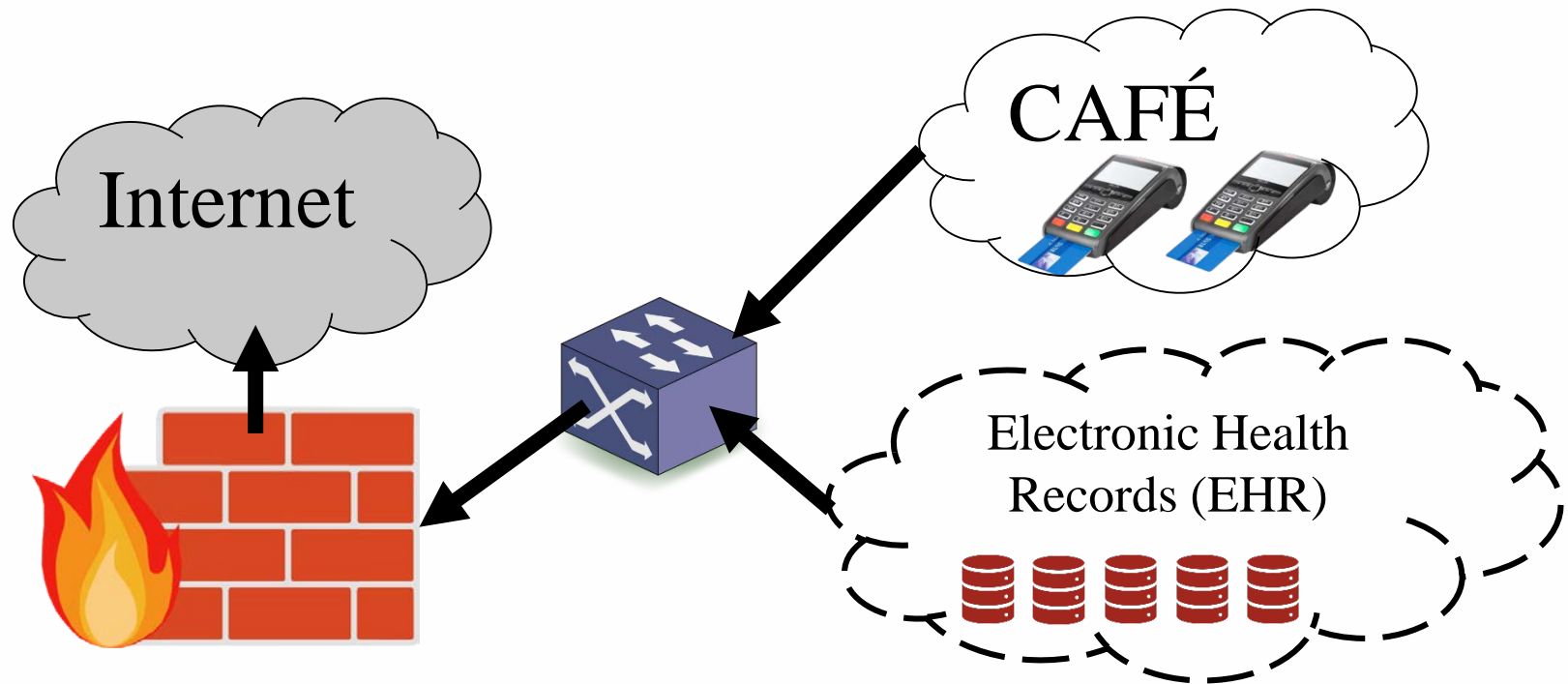
- ▶ Compromise bank accounts and financial credentials
- ▶ Transfer funds to mule accounts
- ▶ Perform ATM jackpotting attacks
- ▶ Conduct mass compromise of debit and credit cards from Point-of-Sale (POS) terminals in large enterprises





Relevance

- ▶ In many instances, POS devices are on the same network as other, more sensitive resources
- ▶ FIN7 has been observed delivering HPH-related lures



Recent Indictments

The indictments allege that three Ukrainian nationals are members of FIN7, identified as:

- ▶ **Dmytro Fedorov (arrested in January 2018)**
- ▶ **Fedir Hladyr (arrested in January 2018)**
- ▶ **Andrii Kopakov (arrested in June 2018)**

The three allegedly contributed to FIN7's years-long reign as one of the most sophisticated, and aggressive, financially motivated hacking organizations in the world.

Each of the three FIN7 conspirators is charged with 26 felony counts alleging conspiracy, wire fraud, computer hacking, access device fraud, and aggravated identity theft.

The three men allegedly had high-profile roles in FIN7:

- ▶ **Hladyr as its systems administrator**
- ▶ **Fedorov and Kopakov as supervisors to groups of hackers**

Wired



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER



Operations

FIN7 Tactics, Techniques, and Procedures → Operations Overview [DOJ](#)

Identifying a Target

-FIN7 targets particularly fast-food and casual-dining restaurants, hotels, casinos, and those with a high frequency of point-of-sale transactions.



-FIN7 gathers information to develop messaging similar to the company's routine business communications.

Grooming

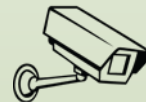
-Spear phishing e-mails target victim company employees: typically public-facing contacts, like employees handling catering requests and reservations, and/or in a managerial position.

-FIN7 accompanies the e-mails with telephone calls to persuade the employee to open and activate the e-mail's attachment, which contains malware.



Infiltrating System

-The malware allows FIN7 to connect to the computer, download additional malware, and move through the company's network. The malware allows FIN7 to conduct surveillance on company employees, capturing credentials to gain elevated network access.



-FIN7 locates the Point of Sale systems containing customer data and steals caches of payment card numbers.



Selling Stolen Cards

Stolen payment card information resurfaces in online underground marketplaces. Purchased card numbers enable criminals to make unauthorized charges to unsuspecting cardholders. Charges may include typical retail purchases as well as the purchase of gift cards.



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

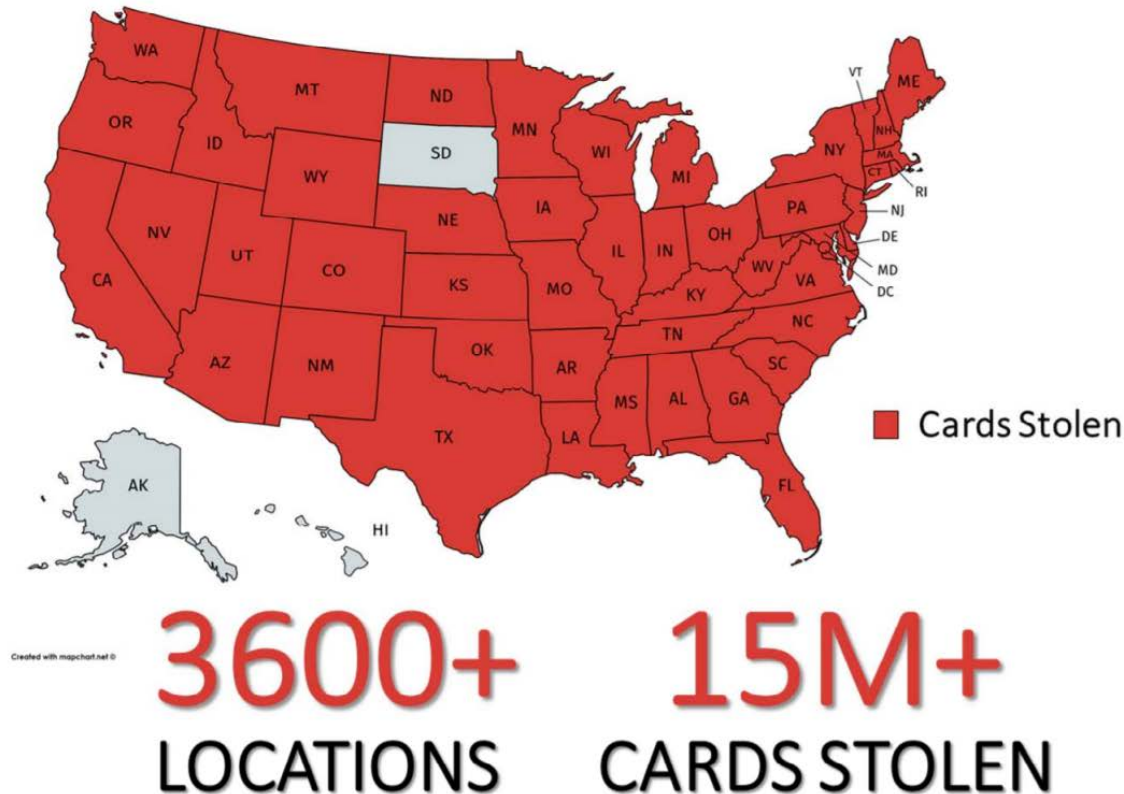
HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

Campaigns

FIN7 Nationwide Impact – DOJ

FIN7 Nationwide Impact



Map depicts business locations that were compromised and had customer payment card data stolen.
These numbers are based on the investigation to date.



Campaign Example

Red Robin Gourmet Burgers ([Wired](#))

27 March 2017

Red Robin employee receives complaint email with attachment from “ray.donovan85@yahoo.com”

“Within Days”

Fin7 had mapped Red Robin’s internal network.

“Within One Week”

Fin7 obtained a username and password for the restaurant’s point-of-sale software management tool

“Within Two Weeks”

- FIN7 member allegedly uploaded a file containing hundreds of usernames and passwords for 798 Red Robin locations
- Network information
- Telephone communications
- Locations of alarm panels within restaurants



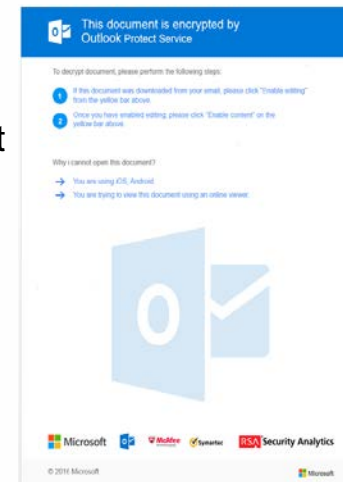


BATELEUR → FIN7 Hallmark (proofpoint)

- ▶ First observed: 2016
- ▶ Last update: April 2018 ([Accenture](#))
 - Minor upgrades from the previous version (1.0.8) but instead included only minor changes, such as the addition of a new network traffic encoding prototype function

JScript Backdoor

- ▶ Delivered via macro-laden Word documents in phishing emails
- ▶ Email messages sent from Outlook or Google accounts
 - Lure document claims attachment is protected OR encrypted by Outlook or Google services, matching the sender domain
- ▶ **Tinymet**
 - BATELEUR downloads a small Meterpreter downloader script
- ▶ Utilizes Powershell password grabber



Targeting

Targeting ([Twitter](#))

FIN7 is characterized by their persistent targeting and large-scale theft of payment card data from victim systems...

Shifting Focus

FIN7's financial operations were not limited to card data theft

- ▶ Pivot to target finance departments within the victim organization (after POS exfil fails)
- ▶ Spear-phishing emails to personnel involved with US Security and Exchange Commissions (SEC) filings at multiple organizations
- ▶ Sought non-public information to exploit in stock trading



Social Engineering

Social Engineering ([DOJ](#)) ([twimg](#))

TTPs

- ▶ Launched numerous waves of malicious cyberattacks on numerous businesses operating in the United States and abroad
- ▶ FIN7 carefully crafted email messages that would appear legitimate to a business' employee
- ▶ Accompanied emails with telephone calls intended to further legitimize the email
 - ***In some campaigns, phone calls before the email***

According to the Indictment...

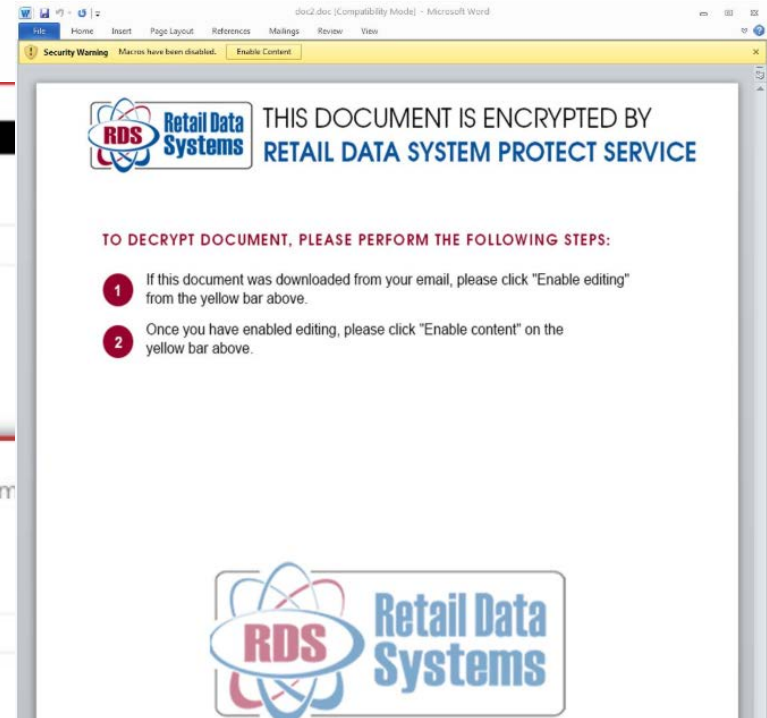
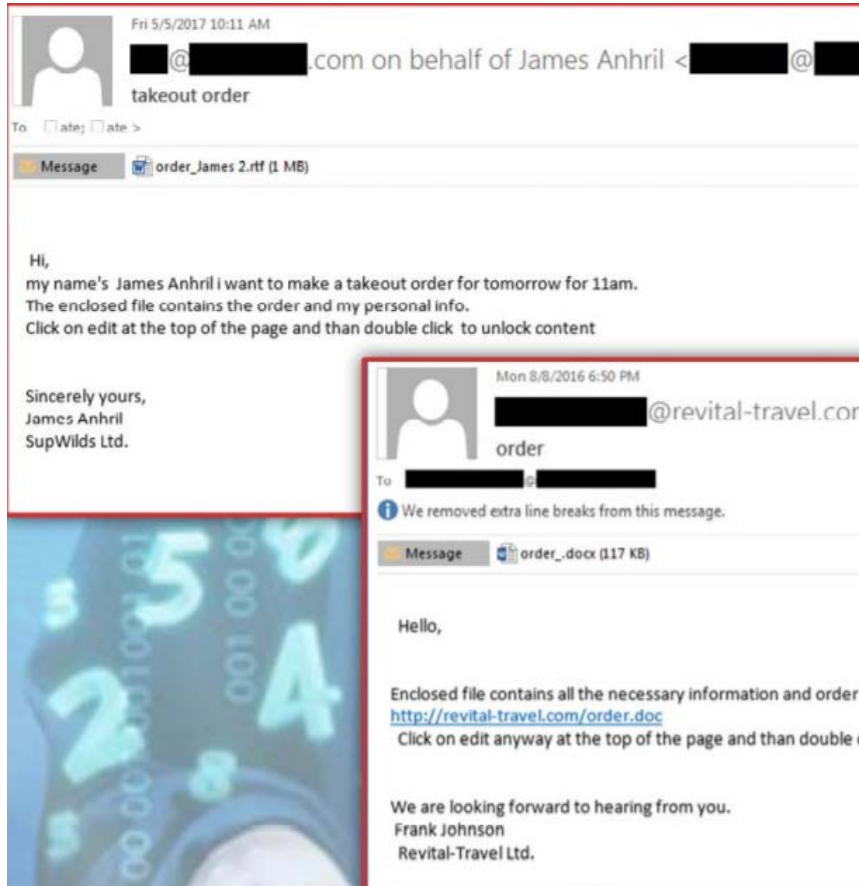
“When targeting a hotel chain or restaurant chain, a [FIN7 operator] would make a follow-up call falsely claiming that the details of a reservation request, catering order, or customer complaint could be found in the file attached to the previously delivered email”



Social Engineering

FIN7 Tactics, Techniques, and Procedures

→ Phishing Emails / Lures DOJ



Social Engineering

FIN7 Tactics, Techniques, and Procedures

→ “FINdigestion” ([FireEye](#))

- ▶ Early 2017 (for over a year)
- ▶ Pattern of email complaints
- ▶ Lodge food poisoning complaints
- ▶ Malicious documents attached

FireEye:

This pattern of detailed complaints eventually expanded beyond individual complaints and into litigious concerns raised on behalf of “the government”

Food poisoning control




Combi Security

Combi Security ([Wired](#)) ([Gary Warner](#))

- ▶ Front Company
- ▶ Hired penetration testers who believed they were working for **Combi Security**
 - Moscow/Odessa/Haifa based company performing legitimate pen-testing services for clients
 - Jobs were managed in JIRA (to track long software development projects, to communicate about the infiltration of their victims)
 - Listed US targets on its website
 - Posts on job sites, including LinkedIn

Recruiters



Martin Kornev
System administrator at Combi-Security

📅 User since June 2016
🔍 Last active: System administrators, 22 June 2016

Company details

Combi Security – one of the leading international companies in the field of information security. Its headquarters are located in Moscow and Haifa.

We – a team of top professionals in the field of information security for all kinds of organizations working around the world. Our main specialization – complex audit projects of any complexity, the delivery of software and hardware.

Our main mission is to ensure the safety of your activities, minimizing the risk of information technologies. Each call to us for help, we consider very carefully on an individual basis, offering the best solution in the framework of the objectives and characteristics of expressed needs.

Web site: <https://www.combisecurity.com/>



Metasploit Developer

Combi Security

Mar 2015 - May 2018 • 3 yrs 3 mos

Haifa, Israel

Improving the functionality of Metasploit Pro for of the customer needs .
Development and improving Metasploit Framework modules.
Development alternative frontend for Metasploit Pro on Ruby on Rails.
Fix various bugs of the Metasploit Framework.
Development Command & Control server on Ruby with transports on HTTPS and DNS.

[Александр \(China Syndrome\) \(@R3dfruitrollup\) Twitter post](#)



Protection & Mitigations

User Education and Training

- ▶ Being able to recognize phishing scams
- ▶ Phone calls before / after receiving an email = **red flag**

IOCs - FIN7's Most Recent Bateleur Malware Campaigns (OTX)

03c6601a7fef76fce7fb63c116ef5fb9
05aa48a9c536ad644a2e91eddf2c0511
1a2e7a9bc8b6e6f359b80173c1f3f42d
298774c49ee2a1e823f8049a34c09609
9c289f5db447ac00069b76ff5f8009d1
aab98b81b9f899183fd090c5f0fe402b
b36782a9a2b34e8385702ec00cb85065
e5614d2eec5d2b75c5eb26e059932f25
e7702f9585616283b6b412b06b274dbf
<http://toshiba.org.kz/robots.txt>.
<https://swift-fraud.com/>
info@apple-istores.com
safe.my-documents.biz
swift-fraud.com
toshiba.org.kz



Conclusion

Upcoming Briefs

- ▶ Exploit Kits
- ▶ Trends in Malicious Macro Usage
- ▶ Cryptomining Landscape
- ▶ Various APT/FIN Groups

Analyst-to-analyst webinars are available

Questions / Comments / Concerns?

HHS HCCIC Email Address: HSHCCIC@hhs.gov

