GLOBAL CONNECTED AIRCRAFT SUMMIT 2019

Facing A Cyber Incident in Real Time – Security Incident Tabletop

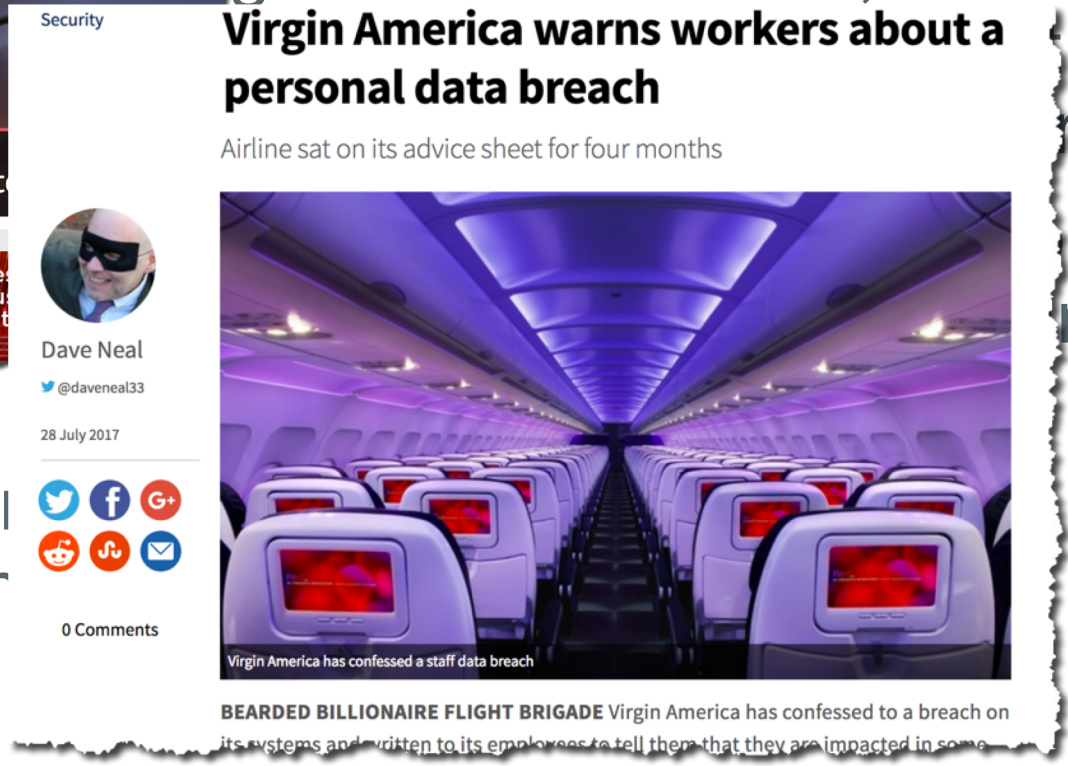
GLOBAL CONNECTED AIRCRAFT SUMMIT 2019

Introduction

- Director of Threat Defense at Alaska Airlines.
- 20 Years of Information Technology experience with 18 years in Information Security.
- Built Threat Intel and Incident Response capabilities for multiple technology companies, including ServiceNow and F5 Networks.
- Lifelong aviation nerd, interested in the convergence of aviation and networked onboard systems.
- Mother to six kids and my corgi, and wife to my partner.

Background

- In g at Alaska Airlines, in week th the Vi r.
- Sp n, ac nd user credentials.
- Worked with external cou to scope the breach, and cor



GLOBAL CONNECTED AIRCRAFT SUMMIT 2019

What is your really bad day?

- Lets walk through an incident and talk about how would *you* respond?
- Use this as a small tabletop, are there processes or procedures that you might not have?
- This session is audience participatory!!! – If you don't participate, I might call on you ;)

Scenario Background

You are an Information Technology Practitioner for an international airline; your airline is primarily US Domestic with flights to Europe and Asia.

You are responsible for detection and remediation of security breaches and incidents, and may call in other team members to assist.

Disclaimer -

The story, all names, characters, and incidents portrayed in this production are fictitious. No identification with actual persons (living or deceased), places, buildings, and products is intended or should be inferred. No animals were harmed in the making of this scenario.

The Story Begins

On Thursday morning you open your email, and receive a notification from the Aviation ISAC that the Las Vegas Airport experienced a ransomware attack on their common use infrastructure. Your airline flies into LAS, so this is a cause for concern.

Users of these airport systems have been cautioned against receiving or opening any executables which may have originated from LAS airport.

The LAS airport has not released complete details or Indicators of Compromise of the attack.

Lock the SOC

On a Friday afternoon you receive a notifica
Flight Operations SOC can no longer acces
They have tried rebooting their machines, b
accessible and when they reboot the mach
message, indicating the system is infected

Shortly later you are notified that flight plan
SMB file shares to move data are no longe
to be dispatched and Flight Operations is re
processes.

Gentlemen!
Your business is at serious risk.
There is a significant hole in the security system of your company.
We've easily penetrated your network.
You should thank the Lord for being hacked by serious people not some stupid schoolboys or dangerous punks.
They can damage all your important data just for fun.
Now your files are crypted with the strongest millitary algorithms RSA4096 and AES-256.
No one can help you to restore files without our special decoder.
Photorec, RannohDecryptor etc. repair tools
are useless and can destroy your files irreversibly.
If you want to restore your files write to emails (contacts are at the bottom of the sheet)
and attach 2-3 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.
Please don't forget to write the name of your company in the subject of your e-mail.
You have to pay for decryption in Bitcoins.
The final price depends on how fast you write to us.
Every day of delay will cost you additional +0.5 BTC
Nothing personal just business
As soon as we get bitcoins you'll get all your decrypted data back.
Moreover you will get instructions how to close the hole in security
and how to avoid such problems in the future
+ we will recommend you special software that makes the most problems to hackers.
Attention! One more time !
Do not rename encrypted files.
Do not try to decrypt your data using third party software.
P.S. Remember, we are not scammers.
We don`t need your files and your information.
But after 2 weeks all your files and keys will be deleted automatically.
Just send a request immediately after infection.
All data will be restored absolutely.
Your warranty - decrypted samples.
contact emails
eliasmarco@xxx.com
or
CamdenScott@xxx.com
BTC wallet:
adjlkjwd2jjjd3i3j33ijdi3jdi3dj3i
Ryuk
No system is safe

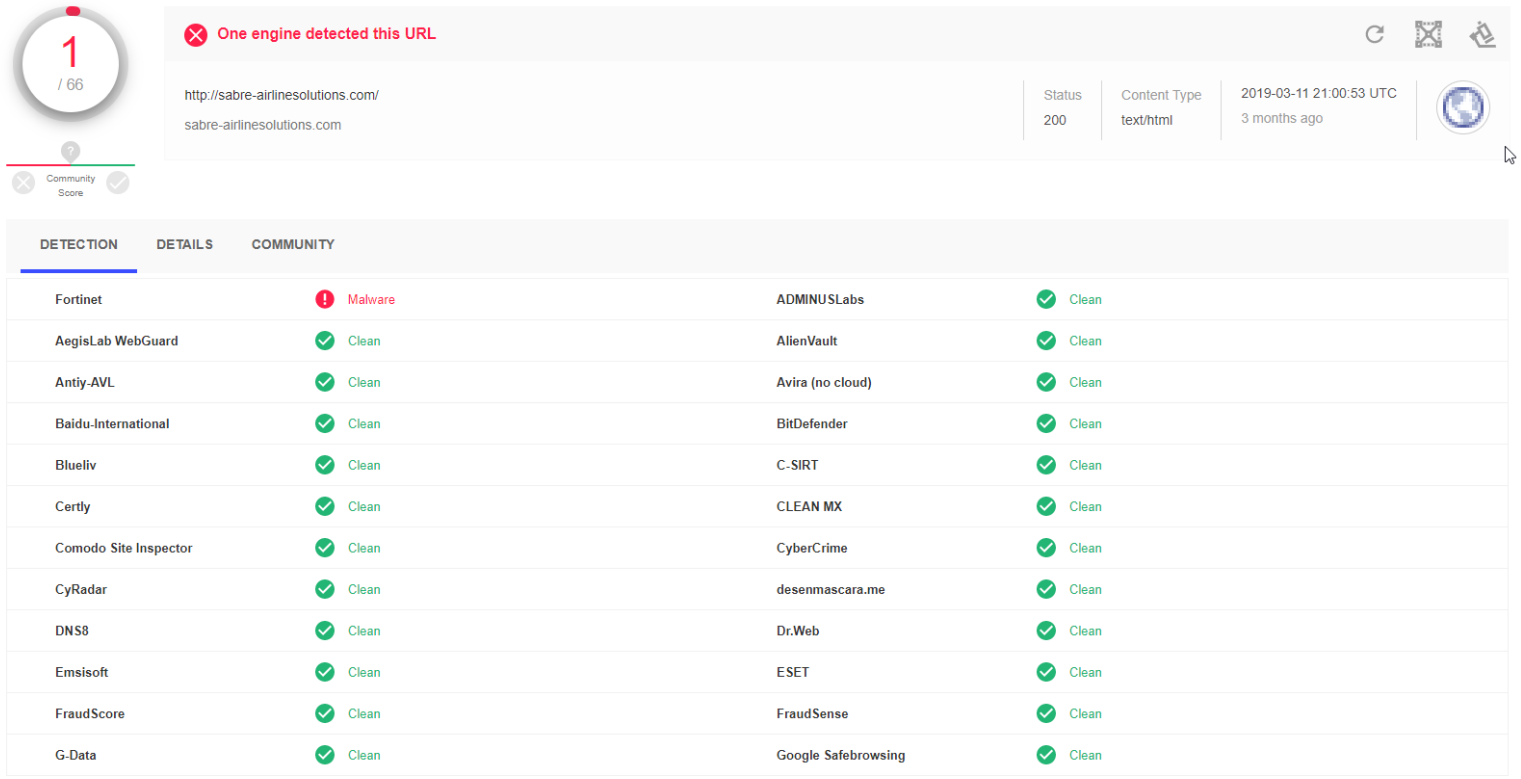
GLOBAL CONNECTED AIRCRAFT SUMMIT 2019

Grounding Flights

Your IT Operations
several flights have
out.

As you conduct fore
the Information Sec
connecting to sabre
does not appear to

Working with your f
the Ransomware is



GLOBAL CONNECTED AIRCRAFT SUMMIT 2019

Round 1 - Complete

After 7 hours of down time, your IT Operations teams was able to fully restore systems and recover full flight operations. Passengers have been rebooked and the airline is starting to resume regular operations. Social media response is swift and harsh from the flying public. Some accounts on twitter, draw the conclusion that this may be caused by a cyber attack.

Fearing the backlash from the flying public, members of Corporate Communications wish to downplay the fact that this was cyber security related incident and want to communicate this event as an IT Outage.

ISAC Outreach

The team from the Aviation ISAC reaches out to you about the outage and you inform them of the ransomware variant that was seen, and the suspicious domain connecting with the sabre.exe file.

Down the Rabbit Hole

Details for sabre-airlinesolutions.com

View:

Severity	Confidence
VERY-HIGH	90

Status	Active
Type	Domain (APT Domain)
Indicator	sabre-airlinesolutions.com
IP	94.156.35.65
Tags	AAG:TI:IOC-HIGH, 19-00002783, Attacker, Cyber-Espionage, iSight, network, New-Domains-Attributed-to-APT39-Exemplify-Continued-Interest-in-Aviation-and-Telecommunications-Industries
Last Modified	2019-02-19 15:35:53
Entries	2
Country	BG
ASN	34991
Organization	Neterra Ltd.
Domain Registration	Name: REDACTED FOR PRIVACY Organization: REDACTED FOR PRIVACY Address: REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, Torun, POLAND, REDACTED FOR PRIVACY Created: 2018-04-28 01:47:03 Last Updated: 2018-12-31 22:51:29
Analysis Links	Google Safe Browsing, URLVoid, VirusTotal, Web of Trust

Edit

New Domains Attributed to APT39 Exemplify Continued Interest in Aviation and Telecommunications Industries

Feb 13, 2019 — 19-00002783, Version: [1]

TURKEY | UNITED STATES | EUROPE | APT39 | CYBER ESPIONAGE | HOSPITALITY | TELECOMMUNICATIONS

Executive Summary

- New infrastructure attributed to Iran-based APT39 is highly suggestive of continued targeting of personal and customer information associated with the aviation and aviation technologies sectors and the telecommunications industry.
- These domains and others that mimic web services may portend to a broader scope of targeting that encompasses Europe, Western Asia, the United States, and possibly beyond.

Threat Detail

FireEye Intelligence recently identified new domains we attribute to Iran-based APT39 that suggest continued interest in the civilian aviation sector, the aviation technology solutions industry, and the telecommunications industry throughout Europe, Western Asia, and the United States. We are unable to determine whether these domains were created to target these specific companies or appeal to others in the verticals.

- The domains are consistent with previously identified infrastructure, masquerade as legitimate web services and software, and represent organizations likely relevant to the intended targets.

A Clearer Picture

Utilizing a list of indicators, you have identify a complete list of systems which have been compromised by the Iranian threat actor, APT39. The systems compromised include several laptops and workstations. ZIP containers used to exfiltrate data were found on multiple systems.

In addition to the RAT installed on the systems, Mimikatz (privilege escalation), and other system enumeration tools and scripts are discovered to be installed on the systems.

A Clearer Picture

Forensic timeline indicates that the patient zero was an IT System Administrator, who was compromised by a phishing email sent by the attacker.

Once the attacker had an initial foothold they used Mimikatz to escalate privileges and gain Domain Admin Access. Once they had domain admin they logged into the domain controllers, and created their own domain admin accounts. Additional RAT's were dropped on strategic systems to maintain persistence.

Logs indicate that the activity mostly occurs during business hour Iranian time.

Burning the House Down

Once a complete picture is put together, you move to eradicate the actor from your environment. A complete list of all of the infected systems is compiled.

Once the list is compiled the team moves rapidly to reimage and rebuild all of the systems, while trying to avoid any more negative reaction from customers.

There is always one…

A webserver in your DMZ runs an IIS web service, and hosts a regulatory technical publications server; it is discovered that the attacker has exploited a vulnerability and uploaded ASPXspy, a web shell, possibly to maintain persistence. In consulting with your Flight Operations team it is discovered this this system is a vendor managed solution and is required to be online for FAA and air frame manufacturer access.

In reaching out to the vendor they acknowledge the vulnerability, and claim that a fix will take approximately 6 months to be produced.

A Clearer Picture

Systems compromised included a reservations database, which contains full passenger PII. Multiple remote access servers utilized by reservations agents, weight & balance load planning systems, as well as an HR laptop with multiple spreadsheets with employee PII data.

Multiple regulations, such as GDPR, CCPA, and various state reporting laws mandate that your company must report these data breaches publicly.

The Wind Down

As you continue through the after math of the burn down and clean up, hundreds of man hours, contracted forensics teams, external council, and millions of dollars have been spent in eradicating the attacker and returning your network to a known good configuration.

How do you prepare for this scenario?

Has talking through this given you any insight into an incident?

GLOBAL CONNECTED AIRCRAFT SUMMIT 2019

Let's Talk Iran

- Iran has been interested in aviation and transportation for quite some time. Two main cells target Aviation Manufacturers and Commercial Operators.
  - Chafer –
    - Aircraft Safety/Maintenance Data
    - Aircraft and Engine Documentation
  - APT39 –
    - Passenger Service Systems

Let's Talk Iran

"Chafer" activity was first publicly identified by the private security firm Cylance in a late 2014 report called "Operation Cleaver". At the time, the global campaign was identified as being broad in scope but included aviation infrastructure such as airlines, airports, and aerospace entities in China, South Korea, Pakistan, Israel, Qatar, Saudi Arabia, the United Arab Emirates, and the United States.

In 2017 Symantec observed a shift in the focus of the Chafer actors; their focus appeared to be more oriented toward the supply chain supporting aviation entities, specifically maintenance and repair, aircraft services, and IT companies and organizations supporting air transport. Of note, Symantec found evidence of Chafer targeting an airline in Africa and an international travel reservations firm.

In May 2018 the UK's National Cyber Security Centre issued an advisory warning of Chafer's targeting of airline passenger systems storing bulk personal data.

Iran Motivations

Iran has an aging commercial air fleet, the planes for their flag carrier, Iran Air, are mostly over 25 years old; compounded with a shortage of replacement parts, Iran has a terrible air traffic safety record.

Iran placed place several orders for new, modern Airbus and Boeing aircraft, however in May of 2018, the Trump Administration withdrew from the Joint Comprehensive Plan of Action (JCPOA) and effectively cancelled all open aircraft orders that could not be delivered in 180 days.

Iran also is politically motivated to keep tap on the travel and whereabouts of their citizens when abroad, for this reason we continue to see attempts by Iran to target airline passenger service systems.

Let's Talk FIN6

- FIN6 is an Eastern European cyber crime group who historically has targeted Point of Sales systems, using malware which scrapes credit card information.
- Recently FIN6 has switched tooling to use more ransomware attacks, leveraged against select, large corporate targets. In particular FIN6 has adopted and used Ryuk and LockerGoga as their primary ransomware variants. This malware is typically deployed using TrickBot and Emotet exploit kits.

Ryuk and LockerGoga

Recently there has been an uptick in ransomware attacks against industrial and aerospace entities. These industrial targets include the aluminum manufacturer Norsk Hydro – infected with LockerGoga on 18 March and airport maintenance vehicle manufacturer Aebi Schmidt infected with unidentified ransomware on 23 April. In addition, the French engineering company, Altran Technologies was probably infected with LockerGoga on 24 January 2019.

As recently as yesterday it was reported that ransomware had stopped production at ASCO Industries manufacturing facilities.