Case Study: The Grinch

Georgia Tech

Case Study: The Grinch

- **Introduction**
- An **overview** of the case
- How **legal attribution** was made
- How a **modern crime ring operates**
- **Lessons Learned**

Georgia Tech

Case Overview

Georgia Tech

Preparation

- **Older SIEM**, but on its way out
- **IPSec VPN** with very good logs
- **Netflow** and **DNS** logging
- **No full packet capture system**
- Beginning roll out of **two-factor** but **only active on grade entry**
- **No Security Operations Center**; Investigations run out of Engineering

Georgia Tech

From: Jimmy Lummis
To: Christopher Craig
Date: Monday, December 1, 2014 10:52AM
Subject: Fwd: The VPN issue I called about

…

How I Found Out

Georgia Tech

From: Christopher Craig
To: Jimmy Lummis
Date: Monday, December 1, 2014 12:23PM
Subject: Re: The VPN issue I called about

I think this is going to end up being a much bigger issue than we realize so far…

What I Found

Georgia Tech

- We knew about the **Phishing message**, and that the sender's **account was compromised**
- The sender had her **direct deposit changed** November 7 and had **contacted payroll** on to have it changed back.
- They asked her to **change her password**, but **never contacted Cyber Security**.
- There was also a **system that should have sent an email** to anyone whose bank account information was changed, **but it was broken**.

It Gets Worse…

Georgia Tech

Our Reaction

- Contacted internal **Executive Incident Response**
- Contacted **FBI** and opened a case
- Notified **users**
- **Reset passwords** on all affected accounts
- Contacted **payroll bank**
- Began watching for **new VPN connections from the same ASNs**.

Georgia Tech

Someone from Malaysia tries the account **we knew about** in the VPN.

It **fails.**

Then they use a new account **we didn't know about.**

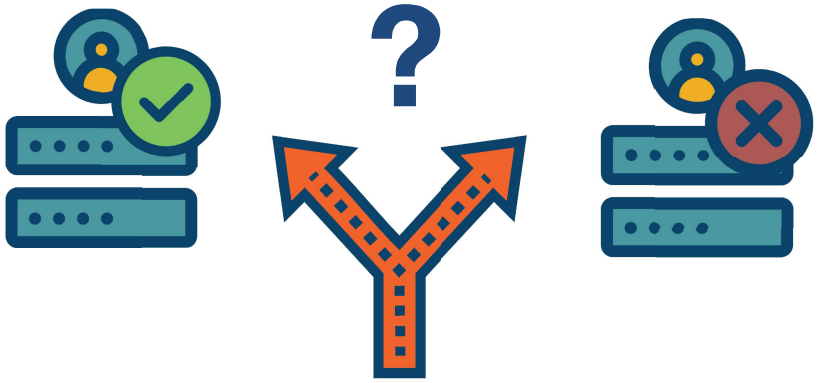
The Next Day

What Next?

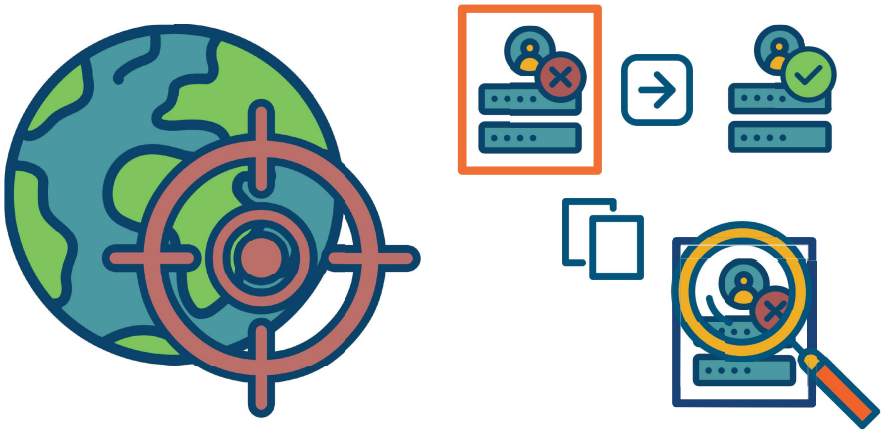
Making Legal Attribution

What Do We Know?

- The actor is staying on the **same VPN account**
- They seemed to **learn about their targets**
- Generally **VPN users didn't have payroll compromised**
- VPN users were **also the lowest paid users**
- The **source IPs** I was seeing had been **seen by others** over the past year
- **Other schools** have had them in the system for months



Which Way to Go?



Tracking the Actor

- Pushed in **VPN logs and IDS metadata** for the affected connections.
- Started **identifying new compromised logins** as fast as he made them.
- Found that the **VPN was logging the client MAC address**, and that it was **consistent** across all of the suspect connections.

```
2014-12-01T03:21:41.556360-05:00 ipsec5.vpn.gatech.edu
%ASA-7-734003: DAP: User ppaul31, Addr 123.136.107.46:
Session Attribute endpoint.anyconnect.macaddress["0"] =
"f4-b7-e2-7b-32-9b"
```

Log Correlation!

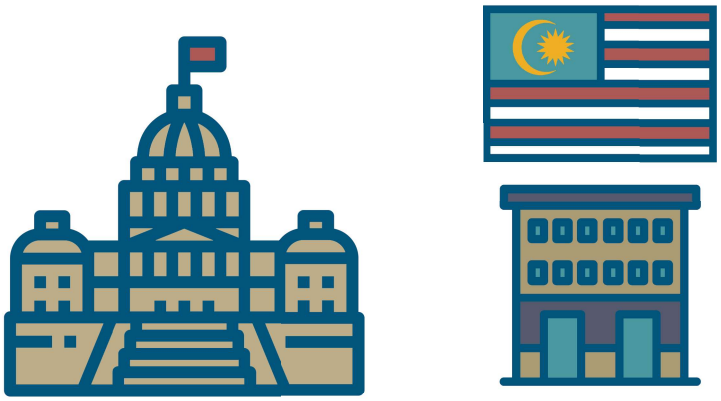
EDU hosts

hostname	event_type
[redacted].edu	tls
[redacted].edu	tls
[redacted].edu	tls
[redacted].edu	fileinfo
[redacted].edu	http
[redacted].edu	tls
[redacted].edu	fileinfo
[redacted].edu	http
[redacted].edu	fileinfo

SIEM Analysis of Outbound Connections

Filing International Charges

Georgia Tech



Filing International Charges

Georgia Tech

Georgia Tech

What Does a Crime Ring Do on a VPN?

Georgia Tech

From: Georgia Institute of Technology

Date: Monday, November 10, 2014 7:16 AM

To: Someuser@gatech.edu

Subject: Message From Georgia Institute of Technology

One(1) new update Click here, to view message.

- Georgia Institute of Technology

How It Started

50 Per Page ⌄ Format ⌄ Preview ⌄ ‹ Prev 1 2 Next ›

uniqueid	Country
0C372657B6	Turkey
0DD7EAA849	Malaysia
1529C4D575	Malaysia
19F1CB1606	Malaysia
1BCAE310FA	Hong Kong Malaysia
1E4FA963A5	Nigeria
22790C6DC8	Nigeria
290F476917	Turkey
29f60b44ca	Nigeria
2AF09E8402	Malaysia
2C45DD79AD	Hong Kong Malaysia
2D344DFEB9	Turkey
2EA4D52E1A	Nigeria
2FFC63DC4F	Nigeria United Kingdom United States

81 distinct MAC addresses from 16 countries

How Many Actors?

Do Not Overestimate the Enemy

From	To	Chat
a_wire	info_s	i go like work with you boss
a_wire	info_s	you into wire right??
info_s	a_wire	yes
info_s	a_wire	you??
a_wire	info_s	i dey do wire, transfer and dating
a_wire	info_s	but need sure contact for wire work
a_wire	info_s	i spam Mexico most time but not getting good resulf
a_wire	info_s	i get singapore drops well

The Gold Mine

From	To	Chat
kathy	info_s	Why is the FBI calling me?
info_s	kathy	What??!?
DELAY		
kathy	info_s	Nevermind, it was about my husband's pension.

A Bit of a Scare

Chat
okay bro
bro i use use the husband and wife ?
their w2?

More Interesting Chats

From	To	Chat
j_1	z65	OK but you have to buy the tools from me
j_1	z65	And then I show you how to do it
z65	j_1	What tools do i need ?
j_1	z65	Rdp smtp emailist scampage Shell
z65	j_1	Lol...How much is everything ?
j_1	z65	Total 100$ with tools and teaching
z65	j_1	So what would you teach me how to spam ?
z65	j_1	If i have to pay you for teaching i dont have buy all the toolz from you
j_1	z65	You should buy the tools because I am the master
j_1	z65	I spam for people bank logins for 500$

Phishing University

- http://financialaid.ucmerced.edu/requesting-tax-transcript
- http://www.unr.edu/mynevadahelp/studentcenter/finances/viewingpaymentsandrefunds
- http://finance.fullerton.edu/controller/accountspayable/
- http://hr.eku.edu/human-resources-forms
- http://now.uiowa.edu/2013/11/w-2-forms-will-be-available-self-service-site

Web Searches

Financial Impact

- Over **700 credentials**
- Access to over **$1 million in paychecks** per pay cycle
- Folders on over **100 institutions**
- Over **2000 W2s**
- **Countless other scams** including credit card fraud, romance scams, retirement accounts, tax fraud, business email…

Georgia Tech

Lessons Learned

Georgia Tech

Keep Your Friends Close

- Make sure your team has **personal contacts on important non-IT units** (HR, Payroll, Risk Management, Controller's office…)
- Have a good relationship with **your bank.**
- **ISAC** was invaluable for security contacts.
- Establish a **relationship with law enforcement** before you need it.

Georgia Tech

How to Talk to the FBI

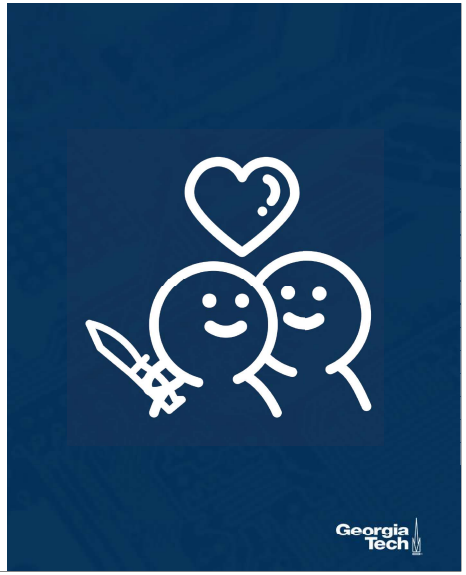
Georgia Tech

Know How Badly You're Hacked

- Know within Information Security **how risk averse** your institution is.
- Understand **your capabilities**
- Be able to **get quick approval to investigate** before starting mitigation.

Keep Your Enemies Closer

- **Don't be to quick to give up intelligence** to block the threat unless you know you're actually blocking the threat.
- Try to **get as much information and share as little** as you can
- **Optimize your workflow** to learn about your adversary as quickly as possible



Don't Cycle Passwords

Our logs show them **retrying the same passwords** about every six months.