CASE STUDY : INVESTIGATION
ULRIC ISAAC DARWIN

Braden Simpson
braden@uvic.ca
V00685500

February 6, 2013

1 INTRODUCTION

Ulric Isaac Darwin(henceforth known as UID), an employee at Domain inc., has brought to the attention of the Investigations Dept. that his email account has been compromised, and stated "Someone has hacked my account."[1] The systems at Domain are implemented with the following:

- Active Directory Authentication
- Exchange Email System
- Outlook Web Access
- PIXIE Email Gateway

2 INITIAL QUESTIONS / INTERVIEW

After UID made the complaint, he was asked:

IT : "Why do you think you were hacked?"

UID : "Because there were emails of my own sent back to me."

Which eluded to the scope of the problem. This means that the system described in Section1 is probably where the attacker was sending the emails, since those are the places that UID's company email can be accessed. Which leads to the following questions:

IT : "What were the subject lines of the emails in question?"

UID : "reluctant mumbling"

UID : "'Sadness vs Happiness', and 'When I win this will you come?'"

The simple fact that UID was reluctant to answer this question tells us that the emails in question are probably from illicit activities for the workplace. Which is our first clue that he might not be as innocent as simply getting his account hacked. From these, the investigation was able to take place.

3 EMAIL LOOKUP

After getting the two subject lines from interviewing UID, the email lookups yielded the results in this table.[2] The emails that are interesting are illustrated in Table 3.

Time	Sender	Recipients	Subject
2013-02-01 6:57	UID@domain.com	ladybird1@yahoo.net	Sadness vs Happiness
2013-02-01 6:57	UID@domain.com	ladybird1@yahoo.net	Sadness vs Happiness
2013-02-01 7:00	UID@domain.com	ladybird1@yahoo.net	Happy Tuesday, Baby
2013-02-01 7:02	UID@domain.com	unknsub@shaw.com	FW: When I win this, will you come?
2013-02-01 7:04	UID@domain.com	unknsub@shaw.com	FW: Sadness vs Happiness
2013-02-01 7:44	unknsub@shaw.com	UID@domain.com	RE: Sadness vs Happiness
2013-02-01 7:44	unknsub@shaw.com	UID@domain.com	RE: When I win this, will you come?

Table 3.1: Emails filtered by the subject line

When looking through these emails we are looking to find any suspicious activity that might explain the attack on UID's account, or, in this case, emails sent back to UID from another source.

The interesting information in Fig **??** is that two emails were forwarded from *UID@domain.com* to *unknsub@shaw.com*, and then *unknsub@shaw.com* responded to UID with those emails. This explains the "returned emails" that UID had seen and reported.
Following this, if Ulric says he didn't send those emails to *unknsub@shaw.com*, then the attacker must have sent them. There are two possibly ways this could have happened, through the corporate domain (at UID's work), or through the Outlook Web Access(OWA) gateway, which is much more likely. Therefore, the next log that should be accessed is the IIS logs for the OWA, provided in the case study[3].

4 IIS LOGS

The IIS logs provided in[3] give us a lot of information, but a lot of noise as well. The IIS logs provide the IP of people logged into the OWA system, the times that

actions were done, the nature of the action(POST, GET, DELETE, PUT, etc). When looking for the emails with subject lines related to the two that UID had said, ie. *"Sadness vs Happiness"*, we find that there are entries for it. There are POST requests for forwarding those emails with an associated IP address, *76.193.130.252*. This is a large step because it places a location and an identity, albeit an indirect one, to the attacker. Looking up that IP address in geolocator service such as iplocation.net[1]. Now that we have an actor (unknsub@shaw.com) and an location(76.193.130.252), we can have just cause to look inside the emails in question. This leads us to the Section 5.

5 Email Contents

The mail headers confirm our suspicion, showing that it was indeed IP *76.193.130.252* that sent the emails, and this time, the email was from *unknsub@shaw.com* to UID.

6 Summary

The interviews revealed that UID was reluctant to give out the subject of the emails, meaning that this he had emotional investment in them, and that they were not work appropriate.

Further investigation into the emails from the mail server showed that there were emails between *UID@domain.com* and *ladybird1@yahoo.com* which were then forwarded from *UID@domain.com* to *unknsub@shaw.com*. Finally *unknsub@shaw.com* emailed *UID@domain.com* with replies to the previous emails.

The IIS logs from the OWA server revealed the IP address that the attacker had, and an IP location service found that IP located in the Saanich Peninsula. In addition, all the emails sent from the OWA access was done in between the time that UID left his house in the morning 7:45am, and the 8:00am, taken from the timestamps on the IIS logs.

7 Conclusions

The nature of the emails that were sent were interesting because they were from Ulric, a male, to a email address ladybird1@yahoo.com, and since the subject of the emails were of potentially sexually suggestive nature, this opens up a few suggestions for motive for people to access those emails, especially significant others. In addition, the ip location was within the area that the wife would have accessed the email account through OWA. As well, the times that it was accessed is in a time that fits the investigation, and finally, the wife would have relatively easy access to the

[1] Service that does lookups on ip addresses and returns various information about that address.

authentication to the OWA account.

There are multiple ways UID's wife could have had access to the authentication to the account. She could:

- Know the password because UID used something that is easy to guess with a good amount of knowledge of him.
- Know the answer to a "forgot your password" security question that UID selected.
- Know the password because he told her.
- The home computer could have login cookies that made the login persist.
- The computer could be set to remember password.

Another possible conclusion, however less likely, would be that someone else in the Saanich Peninsula (assuming the IP is not through a proxy server[2]), somehow got UID's login credentials and sent the emails back themselves. This seems less likely because there is less motive, from the information that we know.

8 Recommendations

8.1 For Ulric

Don't use work assets(Laptops, email accounts, etc.) for inappropriate activities.

8.2 For The Future

- Ensure proper training sessions and reminders for staff of Domain to keep their passwords secret and secure.
- Enforce stricter policies and guidelines for using work assets appropriately.

References

[1] Investigations, "Interviews, Domain Inc," Victoria, BC, Canada. [Online]. Available: http://www.ece.uvic.ca/ henrylee/2013/05/05Investigations-Case.pdf

[2] E. Admin, "Email Logs, Domain Inc," Victoria, BC, Canada. [Online]. Available: http://www.ece.uvic.ca/ henrylee/2013/05/05Investigations-Case.pdf

[3] I. Admin, "IIS Logs, Domain Inc," Victoria, BC, Canada. [Online]. Available: http://www.ece.uvic.ca/ henrylee/2013/05/05Investigations-Case.pdf

[2] Simply put, proxies are ways to route an internet connection through an intermediate connection. See http://www.whatismyip.com/hide-my-ip/what-is-a-proxy/