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."[**?**] 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.[1] The emails that are interesting are illustrated in Fig 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 7:14	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 ?

Figure 3.1: Emails filtered by the subject line

The interesting information in Fig 3 is that the two emails,

REFERENCES

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