Stats & Details

Introduction

The 'malware' is no longer live and there is no way to retrieve it even with a full analysis of an infected document. This is because it pulled from a public Github repository that I controlled. The documents themselves never contained macros (docx files cannot), they stored a link to a macro enabled template.

The Numbers

- 17 breaches
- 11 unique people involved
- 35 total emails with functioning maldocs
- By Dept,
- Dept A - 3/9 (2 people)
- Dept B - 3/8
- Dept C- 4/8
- Dept E- 7/8 (2 people)
- CEO & CFO 0/2

48.5% response rate

Who bit what, no (#) = only one breach

- e (5),l bit G's email (Changes to an upcoming meeting)
- m (2),j bit J's email (UC Berkeley resource)
- m, m, e bit J's email (Policy updates)
- a, d, b bit L's email (Free doughnuts)
- v(2) bit N's email (Policy Updates)

What went right

- Windows based macro just worked. Lots of testing paid off here.
- Every scenario had a decent rate of success.
- Spoofing software worked adequately for the task. Not a flaw with [Organization], SMTP as a protocol was not designed with security in mind.
- A few individuals came forward as soon as were made aware of the phishing attempts, and alerted their departments not to click anything.

What went wrong

- OSX when saving a document removes template links. This broke a not insignificant number of word documents before they ever had a chance. This can be proven by converting the docx to a zip, navigating word -> rels -> and notice that settings.xml.rels is missing. This is the file that stores information regarding templates, and what makes this attack possible. Note for future engagements, do all work and planning beforehand on a Windows machine.
- Make sure all names are spelled correctly. 3 - 4 emails went out with [email missing an s], instead of [correct spoofed email].

Limitations

- Spoofing software either did not allow attachments, or did not allow emails to multiple people.
- Macros were written with Windows in mind, ignoring 40% of the campus runs OSX.
- Self-imposed ethical restraints that a real threat actor may not adhere to.
- An effort was made to keep all information used in emails publicly available.
- Dept Z, Dept X, Dept Y, Dept W, and in general, management was left alone after discovering that the documents would require reinjection. It was already late in the day, and enough data had been collected.
- The emails sent to Dept J, [manager], and Dept K were disarmed before arriving. This is due to an error on my part, not preparing documents carefully enough.

Mitigations

Security Awareness Training
https://dmarc.org/
Remove emails, titles, and nicknames from public facing website. This made writing believable emails completely trivial.

Afterthoughts

There is little to do in the name of security that would not hinder real world use. This attack took 2.5 days of planning, was conducted by an out of practice social engineer, who has never written a malicious macro before. A motivated threat actor could have done significant damage. It is reassuring that the highest profile target hit, was not privileged. This does not put [Organization] in the clear, it only brings to light a limitation of myself. With the insight to prepare every document correctly, it is likely that more targets would have been hit. 48.5% response rate to a spear-phishing attack is not an if, it is a when.