Things to Know about Emotet

Instructions

This training is approximately 8 minutes long. You can speed it up or slow it down using the controls in the player.

For each best practice mentioned, additional resources are listed in the navigation bar labeled "Links" on this webpage. An accessible transcript can be accessed or downloaded from the "transcript" link.

Intro

Emotet is a type of malicious software, or malware, that is downloaded and executed on Windows and MacIntosh operating systems. It is a particular strain of malware that has been continually updated by malicious hackers over the past few years, and those attackers have given it new and powerful capabilities in the form of mass email campaigns that target large organizations, such as university environments, and such as the University of Washington.

Just like other forms of malware, Emotet is often delivered to your computer or other device by way of malicious links or attachments in email. Once your device is infected, it's common for additional malicious programs to be installed. Those programs can be used to steal personal and University login credentials, as well as data on your computer and in your email. It also can be used to deliver ransomware, which locks up your device and makes the data on it inaccessible.

And just like many other forms of malware, if Emotet compromises your machine, it can continue to lurk and steal data through the attacker's "command and control" server until the infection is discovered or the machine or device is completely wiped or reset.

What makes Emotet particularly hazardous is that it can be used to steal several months' worth of email messages, along with your address book. It then uploads, or "extfiltrates" the email and contact information to a malicious hacker's server. Attackers then create fake replies to old correspondence using the body of those stolen messages, and then they send them from what appears to be a known sender with a subject line that is familiar to the recipient because it was previously seen in the inbox. The forged messages often include a link or attachment which downloads an Emotet-infected Office document, and the vicious cycle continues. This spreading method is so effective that several other malware variants, such as Ursnif, have adopted similar methods of spreading through stolen emails.

The primary goal for attackers when infecting a device with Emotet is to create an entry point into the device. Emotet infections are followed up with several other varieties of malware, which may change to suit the attacker's specific goal.

For example, they may follow up an Emotet infection with TrickBot malware if they are interested in surveilling and stealing passwords of a victim. They may follow up with Ryuk ransomware if they want to extort money from the victim in exchange for their files.

At any given time, each of the forms of malware may be mixed, matched, or tweaked to carry out a range of malicious activities, including stealing login credentials, banking and financial information and email contacts and conversations.

One of the more distressing features of Emotet is that it can continue to generate and send email in your name with your old emails even after the infection is discovered and cleaned up on your device. The attacker using their command and control server has a copy of your messages and address book, so they can create new phishing messages and send them directly to other victims without using your computer.

Examples

Let's take a look at some examples.

1. Emotet often uses this formula: here's your name and email address in the name portion of an email header. But it appears in a way that disguises the actual email address.

From: "Familiar Name <email@uw.edu>" <actualaddress@not-uw.com>

Thank you for your help. Please see the attached;
Thank you,
<Familiar Name>
<email@uw.edu>

Here the sender's name appears to be from someone you are familiar with but the actual email address isn't really that sender's address.

2. In this example, the malicious actor has stolen an email thread and tacked on an additional message with a link. If you were to click on this link, you would be directed to a url that would either ask for your login credentials and steal them, download malware--or both.

From: "Familiar Name <email@uw.edu>" <actualaddress@not-uw.com>

We would like to inform you that we have updated invoice to due now/nightly for you.
I have enclosed a copy of the docs for your reference, you can download view using this link:
http://blog.link-to-malware.com/

----- Original Message -----
<Actual prior email correspondence with victim>

3. This example is like the one we just referred to, but it appears to be from an official UW office, in this case, the Office of the Chief Information Security Officer.

From: "Familiar Name <email@uw.edu>" <actualaddress@not-uw.com>

Attached is a copy of the report you requested from the Office of the CISO.
Please find your details below.
http://link-to-malware.co.uk/layouts/

----- Original Message -----
<Actual prior email correspondence with victim>

4. Here is another stolen email thread, with a request to download an attachment that is infected with malware.

From: "Familiar Name <email@uw.edu>" <actualaddress@not-uw.com>

We have updated the invoice format to make the invoice easier for you to read and understand.
Double-click the attached DOC documents to see your Invoice information.
Your details are available on link below.
https://link-to-virus.pl/

We look forward to working with you.

<Familiar Name
ph: 959 <fake-number> ext.7
e:email@uw.edu

----- Original Message -----
<Actual prior email correspondence with victim>

5. This example mixes together a few of the tactics we have just seen. It is a stolen email thread that includes an infected link and prompts you to download an attachment.

From: "Familiar Name <email@uw.edu>" <actualaddress@not-uw.com>

I could not download this document from your link:
http://link-to-virus.com.vn/wp-includes/private-disk
Please check your attachment and send mail again.

Thank you!
<Familiar Name>
Phone (Cell): 672<Fake-number>
Phone (Home): 672<Phony-Number>
e-Mail:email@uw.edu

----- Original Message -----
<Actual prior email correspondence with victim>

So- what do you do?

So- what can you do to protect your computer, devices, email, and your personal and University data?

Here's some tips. For each tip, check the "Links" menu on this web page for additional resources.

1. Use antivirus software on your computer and devices, and keep it updated.
2. Keep your operating systems updated to the latest version and keep them patched with security updates.
3. Think twice before opening any attachments or clicking on any links in email messages, even if they appear to be from someone you trust.
4. Be aware that you could receive Emotet-infected attachments in email appearing to be from a variety of senders, including suppliers, research sponsors, external collaborators, or other University employees.
5. Be aware that these emails may appear as orders or shipping confirmations, delivery status updates, invoices, and holiday greetings, but also be aware that there really is no "typical" appearance for these messages, since they are adapted all the time.
6. If you are ever in doubt about the validity of a message, call the sender to verify that they sent it.

7. Report messages that appear to have malicious attachments or links, or ones that appear to be from spoofed accounts. Find "Report messages" in the "Links" menu to learn how to send suspicious messages as an attachment.
8. If you suspect that your device is compromised, find "Report an Incident" in the "Links" menu for instructions on reporting it.

End & Credits

Thank you for listening and thank you for protecting UW data.