Science Translations
Established 1990
PC410.COM™
PC Updater News

DocuSign Phish Swarm

Reminder: Phishing is email containing bait. The sender wants you to click their link or open their attachment or call their phone number. The hook may be something you want, but more often, it's something you want to avoid: an invoice, a threat to turn off a service, but always something urgent. And once you've clicked, they'll try to capture your email password, or credit card information, or infect your computer.

I've been seeing large numbers of phishing DocuSign emails recently. The 'from' email address isn't from DocuSign.net; it's just some random email. The message itself looks like a DocuSign message, but the request is to view an invoice instead of the usual 'sign an agreement,' which is what DocuSign does. However, when you float your mouse over the link to visit the document, the link that shows is at Google Docs, starting with "https://docs.google.com/..." and leads to a message that

"Previewing is disabled" and there is a link to a random website to download a Microsoft Word file. On opening that safely in LibreOffice or WordPerfect, I see a request to enable active content or macros. Macros are programming code, and they don't belong in invoices.

There is another standard clue: It's addressed generically to "Dear Recipient," and the text itself is very short, and very generic.

In short: Delete all messages claiming to be from DocuSign that link to Google Docs. Docusign is aware of the problem, and has more information here:

https://www.docusign.com/trust/alerts/alert-new-phishing-campaign-observed

False Authority Syndrome

The fake DocuSign invoices are yet another variation of false authority syndrome. These are the characteristics of false authority messages:

- False: It's from a known company, so it's real.
- False: A famous person says the product will really do ___, so click that link.
- False: A cable news network says something unexpected, and you have to

know now.
- False: A government agency says ‘do this now’.

It’s just a lie to get you to open a dangerous email, or online, it’s clickbait to send you to a website with dangerous content.

Paying a Ransom Also Means Paying the US Government

Ransomware isn’t what it was; it’s worse, again. At first, it encrypted a computer and demanded a payment to (allegedly) decrypt it. Then it would encrypt an entire network, and then ask for a much larger payment to decrypt it. (Again, decryption does not happen reliably.)

The next addition was targeting ransomware at specific categories of public businesses, most notably schools and hospitals, because if you have an email hoax that works on one school, try it on other schools in the same district; they probably have the same security in place.

Now, there is ransomware that uploads data to the attacker, so that the ransom is to get your data back and also not have it published online or sold to competitors. Of course, paying that ransom does not mean those extra steps, possibly profitable on their own, won’t also happen. It’s not like anyone receives a legal ‘certification of data destruction’ and a receipt after sending Bitcoin ransoms to an unknown group with no known location.

Of course, everyone who pays the ransom, whether they get their data back or not, whether they saved their data from publication or not, is making ransomware more profitable and popular in the darkest parts of the internet. Paying it, supporting crime, is a bad idea in general.

And now the US Treasury Department is warning that there may be fines for companies who pay these ransoms, or assist in paying them. The computer press is saying that paying a ransom leads to a fine. It’s slightly more complex than that; such actions would require legislation. The Treasury Department’s statement says that penalties apply for doing business with companies, countries, or persons on their sanctions lists. We’ve had that limitation on imports and exports for decades, specifically the list of countries that we can’t do business with. Here it is:

https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information

The problem is that doing business with an unknown ransomer means that you are sending money, OK, almost untraceable and completely unrefundable and virtual Bitcoins, to an unknown country, which could be, and most likely is, in a country with no laws against ripping off other countries. So a ransomware payment may be in violation of the sanctions programs and subject to fines.

Here's the press release from US Treasury:
https://home.treasury.gov/news/press-releases/sm1142

So far, I've seen no reports of actual penalties. I suspect that when the fines begin, they'll be combined with negligence claims for very large firms that have associated losses for clients.

Swiss Cheese Security Methods

Protection from ransomware includes multiple layers of security. Recognize that any security method has holes. It's like swiss cheese. You just have to make sure that the layers of swiss cheese overlap so that all of your bread (cash, data, stuff) is protected. Here are the basic layers. More layers of protection exist, but mostly apply to very large companies:

- Employee Training: Recognizing bad emails. This newsletter can be sent to your entire staff, on request, to help with security training.
- Employee Limits: No users should be using Admin-level accounts in Windows. And important data on your server should be limited to only the staff that actually need to work with it. It's not about what they can do, but about what the software that they might click on would have access to.
- AntiVirus Software: It's now usually called endpoint protection. PUP protection ('potentially unwanted programs') must be turned on.
- Patching: All software that uses the internet needs regular patching.
- Windows Updates: Microsoft has made this difficult to break, but the Windows Version should now be no older than 18 months. (Run winver from the Start menu to check.)
- Backup Documents: Backup documents to the cloud, using a service that does not allow ransomware to alter or delete files. Backup services that keep all previous versions of each file are ransomware resistant. Cloud storage systems that store files online for sharing, like OneDrive, Dropbox, or Google Drive, are not resistant, and are not a backup.
- Backup Windows and Software: Create system backups on a schedule. In most cases, keep the last three complete backups.

Overall, planning for ransomware recovery is like planning for a drive failure. I generally replace the drive and restore a backup, because I don't want to attempt cleanup of a drive where every folder has been tampered with, most software no longer loads, and where all the drive contents are suspect.