Indicators of Compromise - Reference Materials

As an update to the FAQ posted on 5/16/2017 regarding the recent phishing incident, we wanted to share even more detailed information to enable you to protect your organization.

This document contains a list of Indicators of Compromise (IOCs) which can be used by Enterprise IT and Security teams to scan for and detect any malicious traffic related to this campaign.

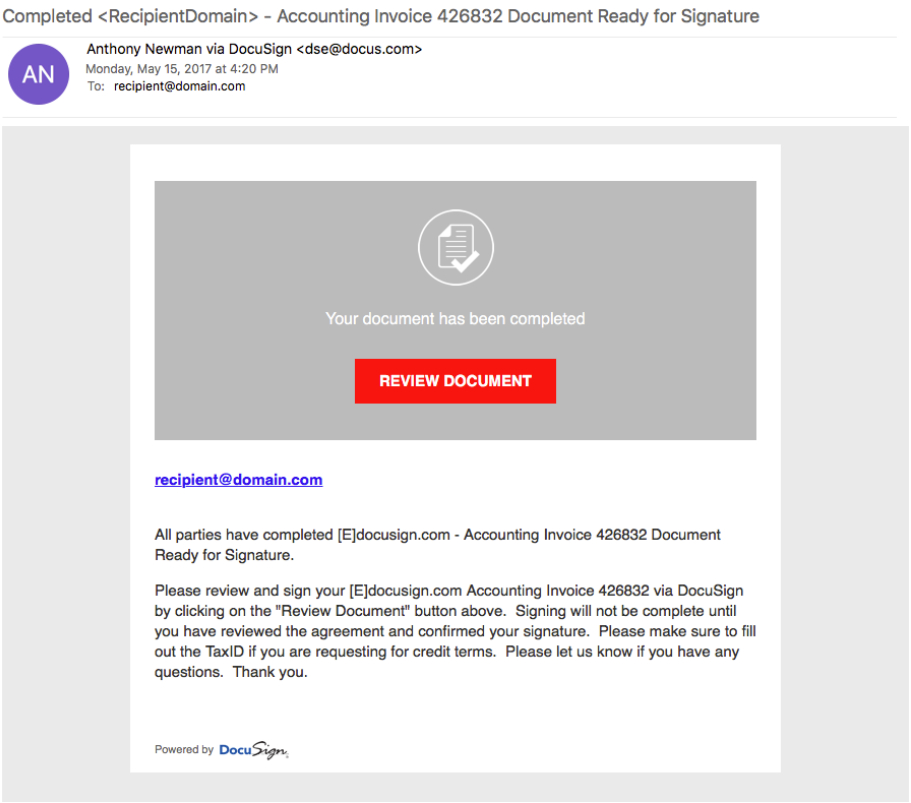
An indicator of compromise is a file, network connection, process or any other trait that may point to a case of malware on a system or network.

1. Phishing Email

The starting points for the two recent campaigns were DocuSign-themed phishing email. A screenshot of this can be found below.

IOCs:

- Sender Address: dse@docusgn.com
- Sender address: dse@docus.com
- Subject: Completed <recipientDomain.com> - Accounting Invoice 426832 Document Ready for Signature
- Subject: Completed: <recipientDomain.com> - Wire Transfer Instructions for <recipient> Document Ready for Signature



2. Files

If a recipient clicks on the link in the phishing email, a Word Document will automatically be downloaded. In order to initialize the malware, the recipient will need to open the Word Document, and enable Microsoft Office Macros. Note: Macros may be handled differently depending on the organization. If macros are enabled by default, then the malware will run once the document is opened. In most situations, the user will need to click the "Enable Macros" option on a banner across the top of the document.

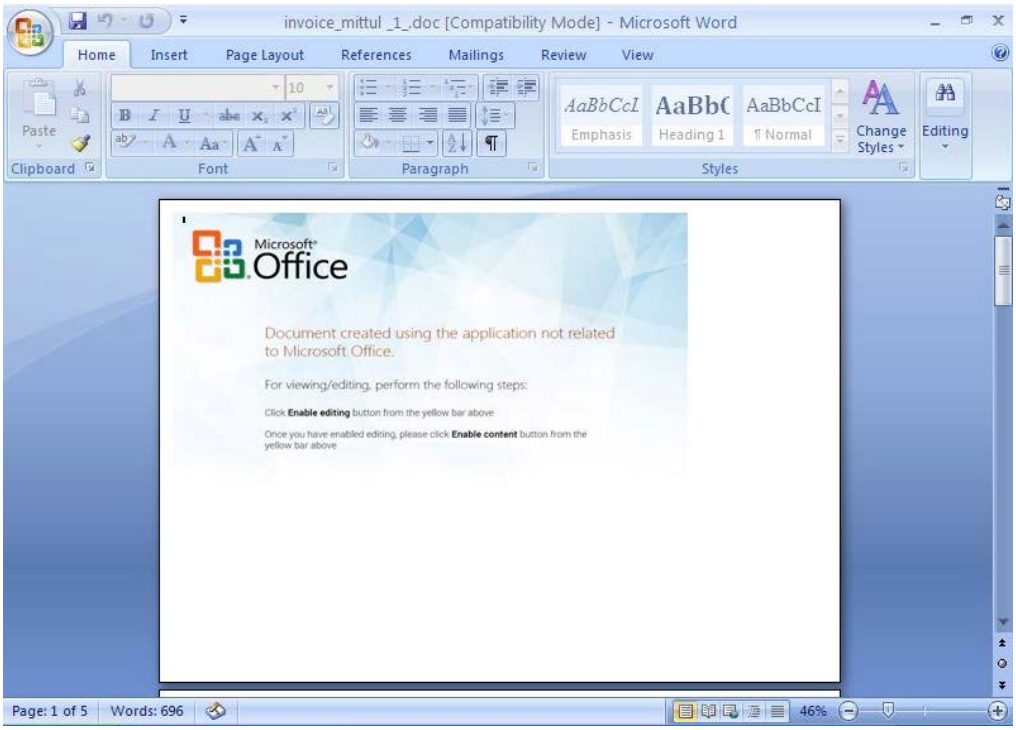
File names and hashes can be found below.

Filename: accounting_invoice_<RecipientName>.doc
MD5: 3c28575aa851aff63114d1a004809f5e
SHA-1: e7fbcb3af663efa4a809ddb9d75942d034addb25
SHA-256: 913a1d8ab2b62a59561bdcf58f505522184259ebdfa9b034289edafdadb0eb64

Filename: Wire_Transfer_<RecipientName>.doc
MD5: d168269c3e7cd006d73c39c2d49106eb
SHA-1: cb6797ff6eb43748c07faaa7bf949a42929a5220
SHA-256: fff786ec23e6385e1d4f06dcf6859cc2ce0a32cee46d8f2a0c8fd780b3ecf89a

Filename: pony.dll (actual name will vary)
MD5: 9c894a6850fdd3fc49cfe1de29558ab0
SHA-1: da1a8b2e6ed101fc3d6092acbb2e5afd04d4620a
SHA256: 437351c9ae0a326ed5f5690e99afc6b723c8387f1ed87c39ebcce85f9103c03a

Filename: evilpony.dll (actual name will vary)
MD5: a498e1a9206d0c976e3544b65a266b9c
SHA-1: ee5f27703fd2caf294b3d9834009c95e804e997d
SHA256: 5bcd2d8ed243d6a452d336c05581291bc63ee489795e8853b9b90b5f35c207d8



3. Malicious Domains

This list contains dropper sites used to deliver the malicious .doc file, and Command & Control (C&C) servers used to communicate with the malware, and deliver additional malicious content. The initial Word Document delivered Hancitor which will proceed to download Pony, EvilPony and ZLoader.

Dropper domains (in bold, below) are found in the phishing email, and all have the following format:<MaliciousDomain>.TLD/file.php?document=MTIzNHJlY2lwaWVudEBkb21haW4uY29tNDMyMQ==

The Base64 document parameter at the end of the URL acts as an identifier for the recipient, and once decoded shows as: 1234recipient@domain.com4321

Domain	IP Address
hudsonhughes.com	184.168.221.32
precisionexposures.com	184.168.221.36
PARTNERSPROJECTINC.NET	184.168.221.38
knoxvilleupholstery.com	184.168.221.46
GODISIMNOT.COM	184.168.221.54
andsihowdint.ru	47.91.90.51
hertretletan.ru	47.91.90.51
rewthenreti.ru	47.91.90.51
boatingflagpole.com	47.91.90.51
hbc-advisors.com	50.63.202.32

Domain	IP Address
zariyamatrimony.com	50.63.202.49
PARTNERSPROJECTINC.COM	50.63.202.53
geheppauld.com	NOT RESOLVING AT TIME OF DETECTION
tannareshedt.ru	54.213.18.155
LIFEIMPACTBYDESIGN.ORG	54.213.18.155
docusgn.com	50.63.202.15
civerusemuch.ru	NOT RESOLVING AT TIME OF DETECTION
noaninghedled.ru	NOT RESOLVING AT TIME OF DETECTION
codybraithwaite.com	69.90.66.240
eventienozze.com	62.149.128.157
heiligerlee.eu	5.200.9.5
adanaokiser.com	93.89.231.87
arabianred.com	107.180.119.182
websitepepper.com	46.17.1.250
wadidncise.com	NOT RESOLVING AT TIME OF DETECTION
parrephetit.com	NOT RESOLVING AT TIME OF DETECTION
anddawassrab.ru	NOT RESOLVING AT TIME OF DETECTION
daletrefhert.ru	NOT RESOLVING AT TIME OF DETECTION
eventsinbutbi.com	NOT RESOLVING AT TIME OF DETECTION
forttehowke.ru	NOT RESOLVING AT TIME OF DETECTION
hanjusrancal.com	178.208.88.117
hapwassparly.ru	NOT RESOLVING AT TIME OF DETECTION
hathenketjohn.com	NOT RESOLVING AT TIME OF DETECTION
hesdirohim.ru	185.22.173.111
kinrinhiked.ru	NOT RESOLVING AT TIME OF DETECTION
muchronnotold.ru	NOT RESOLVING AT TIME OF DETECTION
onewithbohert.ru	NOT RESOLVING AT TIME OF DETECTION
rectincasof.com	NOT RESOLVING AT TIME OF DETECTION
rewtorshosin.ru	46.8.29.202
rigakeddo.com	NOT RESOLVING AT TIME OF DETECTION
riranughone.com	NOT RESOLVING AT TIME OF DETECTION
tancoatthen.ru	NOT RESOLVING AT TIME OF DETECTION
tofhadjustling.ru	NOT RESOLVING AT TIME OF DETECTION
toldhapsinspar.com	NOT RESOLVING AT TIME OF DETECTION
tothecktitres.com	NOT RESOLVING AT TIME OF DETECTION
ughrytitter.ru	NOT RESOLVING AT TIME OF DETECTION

Domain	IP Address
wilnakinhar.ru	NOT RESOLVING AT TIME OF DETECTION
witjowronme.ru	91.226.93.14
SEARCH4ATHLETES.COM	185.48.238.65
PAYSIS.NET	NOT RESOLVING AT TIME OF DETECTION
cheapbillpay.com	185.48.238.65
sitthegemuch.ru	185.48.238.65
LASVEGASTRADESHOWMARKETING.COM	185.48.238.65
LIFEIMPACTBYDESIGN.ORG	185.48.238.65
UN-BANKED.COM	185.48.238.65
marinevenghan.ru	185.48.238.65
tannareshedt.ru	54.213.18.155
LIFEIMPACTBYDESIGN.ORG	54.213.18.155
docus.com	74.117.221.72
mafeforthen.com	164.132.138.136
foarlyrow.com	77.73.68.159
mindsonvacation.com	98.129.229.142
hargotsinlitt.com	178.208.81.27
athinropro.ru	31.41.44.158
forthatenron.ru	212.116.113.247
meiguofeibo.com	98.126.55.34
decorastudio.com	23.98.66.125
salteraero.com	98.129.229.208
andrewjordanpmp.com	162.210.101.144
ok-toys.ru	78.110.50.106
daletrefhert.ru	NOT RESOLVING AT TIME OF DETECTION
fehedthethep.com	NOT RESOLVING AT TIME OF DETECTION
heckgwassehan.com	NOT RESOLVING AT TIME OF DETECTION
hescotirin.ru	NOT RESOLVING AT TIME OF DETECTION
lactalhedttin.bit	NOT RESOLVING AT TIME OF DETECTION
orheckledtit.ru	NOT RESOLVING AT TIME OF DETECTION
rolorretheck.ru	NOT RESOLVING AT TIME OF DETECTION
supspvehisar.com	NOT RESOLVING AT TIME OF DETECTION
toldhapsinspar.com	NOT RESOLVING AT TIME OF DETECTION
ughrytitter.ru	NOT RESOLVING AT TIME OF DETECTION
zithuasnothar.ru	NOT RESOLVING AT TIME OF DETECTION

References

https://malwr.com/analysis/MGM0M2Q5YjQzYThmNDI5NDhiMGJlMjgzNGIwYzc4ZTA/

https://techhelplist.com/spam-list/1141-2017-05-15-completed-domain-accounting-invoice-document-ready-for-signature-malware