Chain 365

Cyber Threat Intelligence

Enterprise & Cyber Security

August 2017

shaping tomorrow with you

Fujitsu Cyber Threat Intelligence – Office 365

Supply Chain Compromise

Global Impact

Contents

Executive Summary

Fujitsu Cyber Threat Intelligence have identified chain phishing attacks affecting Office 365 customers. A range of services are available within Microsoft's O365 platform, including Skype, Office, OneDrive and SharePoint which all allow consumers to access productivity services referred to as SaaS (Software as a service). The availability of these services offers a significant benefit to most organisations in that access is available wherever they require it. However, along with the benefits comes risk, and a number of threats.

Fujitsu CTI research has identified numerous intrusions into organisations by successfully compromising legitimate credentials via Microsoft Office 365 (O365) chain phishing.

This article seeks to highlight the serious risks associated with cloud services if not appropriately managed, monitored and secured, and the potential to further compromise a customer's supply chain.

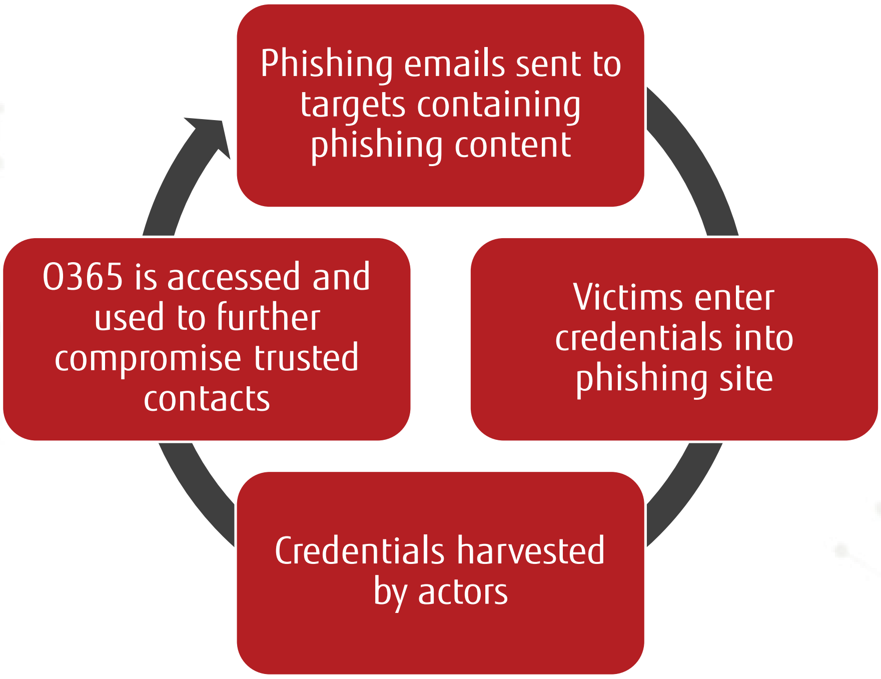
As observed by the recent global ransomware incidents, the impact to supply chains has been significant with, for example, Maersk stating expected losses of $300m as a result. In 2013 the intrusion into Target was as a result of a third party resulting in the theft of millions of credit and debit card records. The net result was over 100m affected customers, and resignation of the CEO and a 4% transactional loss for the year.

Fujitsu CTI have previously highlighted research into cloud security and the risk of unsecured data to both the company and their supply chains as a result of preventable risks - http://blog.uk.fujitsu.com/information-security/mongodb-ransom-attacks-could-you-be-at-risk/

Chain 365

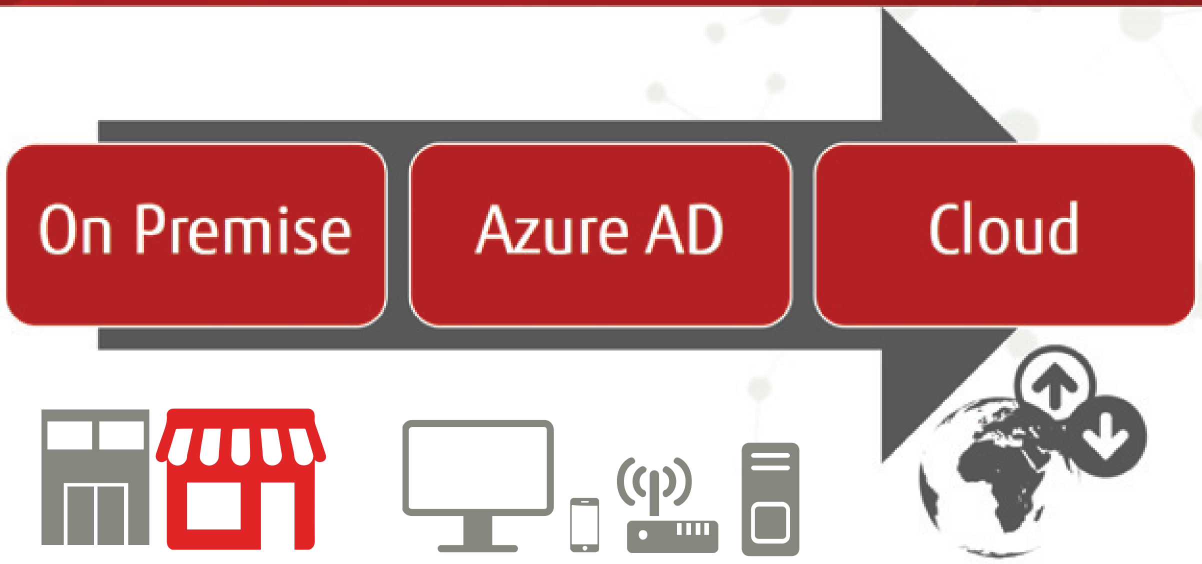
The chain phishing attack, has compromised organisations since at least June 2017. Organisations receive a phishing email from an organisation in their supply chain with a landing page to input Office 365 credentials. The second phase of the attack uses the compromised credentials to force phish further internal and external contacts via a different landing page. The attacks have a higher chance of success as they are from a legitimate user.

The following high-level diagram highlights the attack chain:


Phishing emails sent to targets containing phishing content
Victims enter credentials into phishing site
Credentials harvested by actors
O365 is accessed and used to further compromise trusted contacts

Potential impact

Whilst phishing is not a new concept, and is frequently used as an attack vector to compromise web based services, the risk is amplified to Office 365 customers as compromising and using legitimate credentials allows for access to other Microsoft services within an O365 environment such as Skype, SharePoint and One Drive.



The following table highlights a number of the high-level findings from this assessment

Area(s) of exposure	Potential Risk
SharePoint	Sensitive document library / IPR / Data Loss
Yammer	Community discussions / Data Loss
Skype For Business	Business conversations / Meeting eavesdropping
Exchange	Sensitive email communications / Diary entries
Dynamics	Customer data and ERP
Azure AD	Identity data / credential theft / Domain compromise

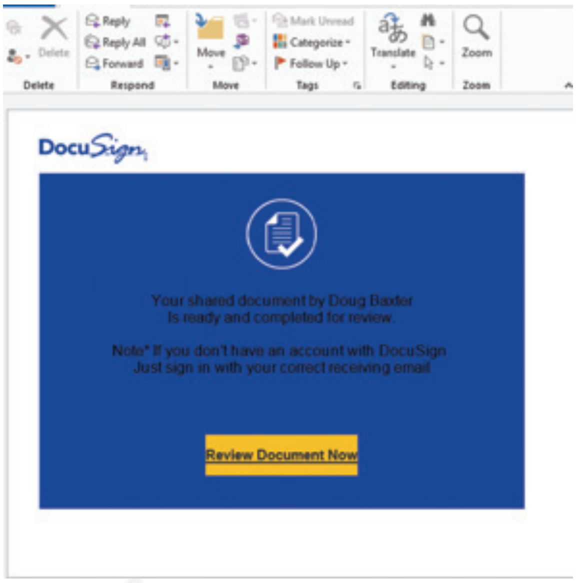
Modus Operandi

Following the analysis of a series of phishing emails and lures, using both DocuSign and spoofed O365 login pages, it has become evident that a significant, and far reaching, attack will most likely be impacting other organisations.

The threat impacts not only the organisation but its supply chain and also, potentially, its client base.

A successful phishing lure, targeting an O365 user, will start a series of events via a chain methodology.

1. Users are sent an email containing a link, disguised in a number of ways

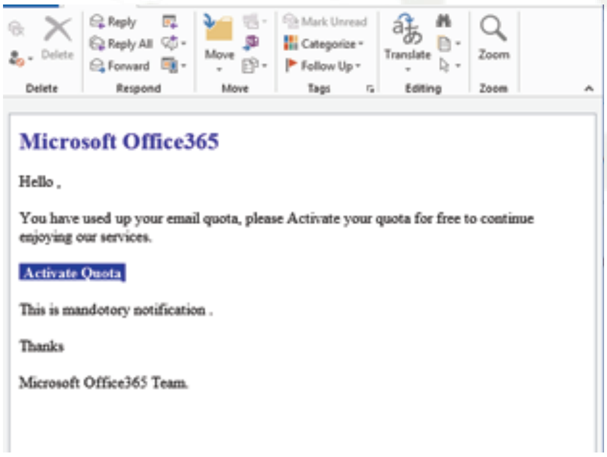


DocuSign

Your shared document by Doug Baxter
Is ready and completed for review.

Note* If you don't have an account with DocuSign
Just sign in with your correct receiving email

Review Document Now



Microsoft Office365

Hello ,

You have used up your email quota, please Activate your quota for free to continue enjoying our services.

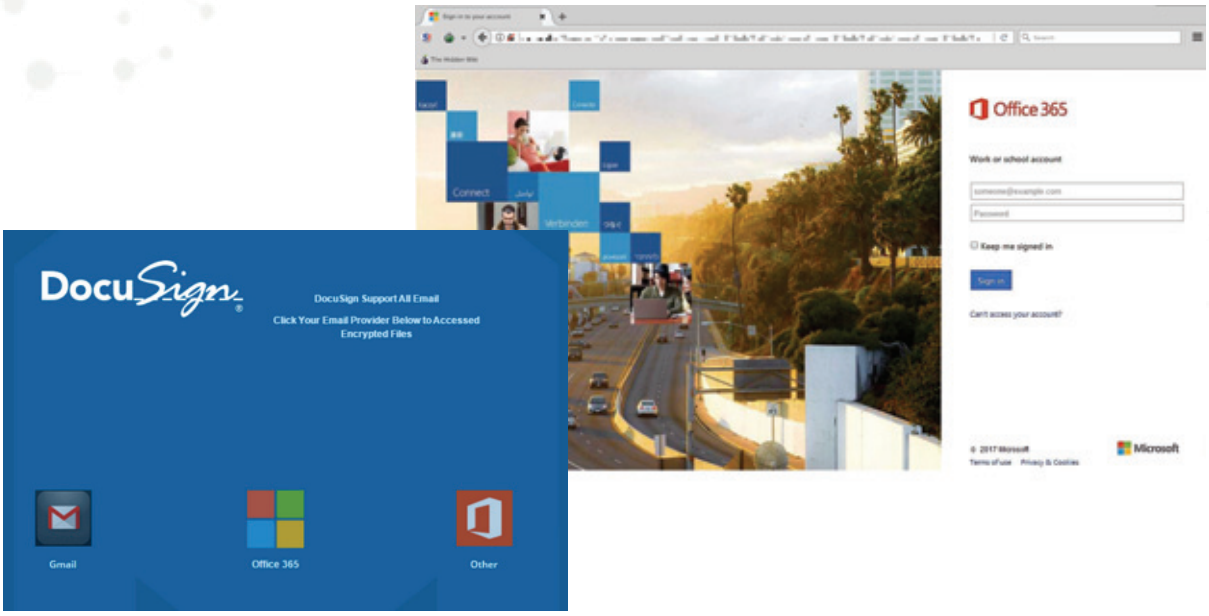
Activate Quota

This is mandotory notification .

Thanks

Microsoft Office365 Team.

2. Users visit the links which commonly reside on, or redirect through, compromised legitimate websites.



Office 365

Work or school account

someone@example.com

Password

□ Keep me signed in

Sign in

Can't access your account?

© 2017 Microsoft

Terms of use Privacy & Cookies

Microsoft

DocuSign

DocuSign Support All Email

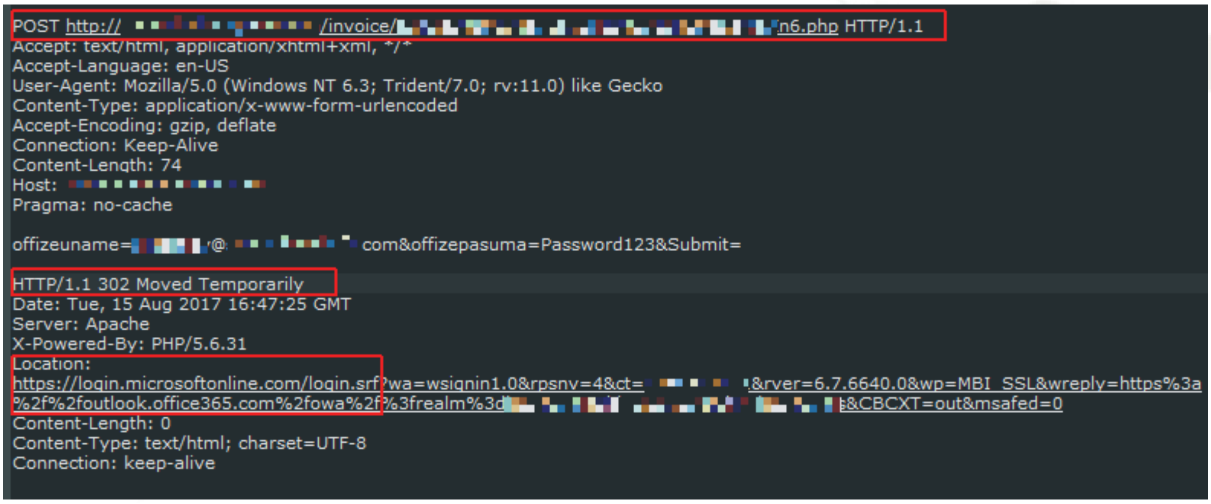
Click Your Email Provider Below to Accessed Encrypted Files

Gmail

Office 365

Other

3. Users enter their credentials and are then redirected to the original Microsoft login page.



```
POST http://[redacted]/invoice/[redacted]n6.php HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Connection: Keep-Alive
Content-Length: 74
Host: [redacted]
Pragma: no-cache

offizeuname=[redacted]@[redacted]com&offizepasuma=Password123&Submit=

HTTP/1.1 302 Moved Temporarily
Date: Tue, 15 Aug 2017 16:47:25 GMT
Server: Apache
X-Powered-By: PHP/5.6.31
Location:
https://login.microsoftonline.com/login.srf?wa=wsignin1.0&rpsnv=4&ct=[redacted]&rver=6.7.6640.0&wp=MBI_SSL&wreply=https%3a
%2f%2foutlook.office365.com%2fowa%2f%3frealm%3d[redacted]&CBCXT=out&msafed=0
Content-Length: 0
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
```

4. The threat actor uses the credentials to then either login to the companies O365 environment, or to configure an external client if Outlook Anywhere is enabled.

5. Threat actor now appears as the compromised user using their legitimate credentials and mass mails a new phishing campaign to known internal and external contacts.

    a. If a recipient queries the email by using Skype, or other communication methods, the attacker can respond, posing as the original sender, to further add legitimacy and confirm the mail is genuine.

6. Recipients, either internal to the organisation or external 3rd parties, then fall victim to the phish as the mail is from a trusted source and proceed to enter their credentials into new, spoofed websites.

7. The steps are repeated both in the same organisation and any external organisation, which provides another continuing link in the chain.

The threat actor can choose who to target and how to target them. This can extend to Business Email Compromise and pose a risk of financial loss to an organisation. Evidence supports this due to the nature of the mails with subjects typically received by financial teams.

Summary

Given the potential access to data stored in O365, the ability to interact with both internal and external users posing as a trusted individual and the onward chain of infection, highlights the serious potential damage this attack can cause.

This attack is successful due to the mail being sent by a legitimate individual. If someone has had contact with an individual they are far more likely to trust and interact with content they provide. Given the ability in this attack scenario to further communicate via Skype this could easily sway even tech savvy users to let their guard down.

The complex configurations Microsoft provides offer numerous remediation steps and configurations against potential compromise.

Fujitsu CTI offer an initial compromise assessment service in which a technical assessment can help determine whether the O365 environment has been compromised through misconfiguration issues, by analysing logs to search for Indicators of Compromise.

Please contact Fujitsu pre-sales team on: securitysalesdesk@uk.fujitsu.com

i	**Technical indicators are available upon request**

Fujitsu Commercial Statement

Accuracy: Fujitsu endeavours to ensure that the information contained in this document is correct but, whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.

Non-Disclosure: The information contained in this document is confidential and is submitted by Fujitsu on the basis that the customer will use it solely for the purposes of understanding their current security risks. The customer may permit those of its employees, advisers and agents having a need to know the contents of this document to have access to such contents, but shall ensure that such employees, advisers and agents are bound by the customer's obligation to keep it confidential. Subject to that, the contents may not be disclosed in whole or in part to any third party without the prior express written consent of Fujitsu. The customer's acceptance of these obligations shall be indicated by the customer’s use of any of the information contained in this document.

Copyright: © Copyright FUJITSU 2017. All rights reserved. Other than for the purpose of evaluation, as set out under "Non-disclosure" above, no part of this document may be reproduced, stored or transmitted in any form without the prior written permission of Fujitsu.

Validity: It is not an offer capable of acceptance and any agreement will require a formal written contract.