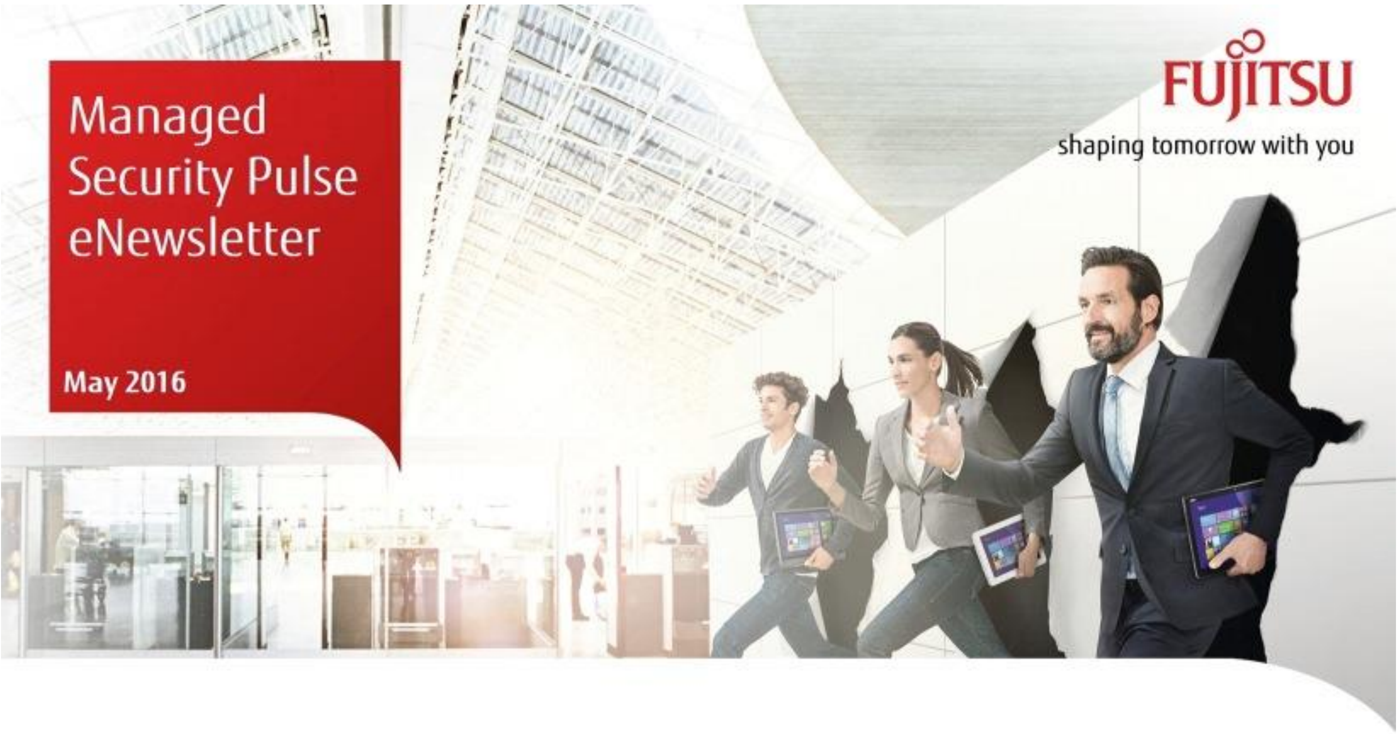


Managed Security Pulse eNewsletter

May 2016

FUJITSU
shaping tomorrow with you

SOC Threat Advisory Threat Level - WARNING

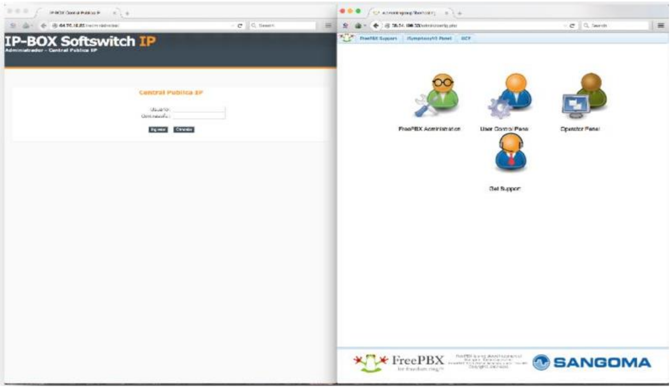
Dridex Phishing campaigns

Phishing attacks seeking to obtain personal or financial information by persuading the user to open attachments or links allowing for the delivery of a further malicious payload

Synopsis

The SOC have been monitoring Dridex phishing campaigns across our customer base over a period of time. Evolving variants of the campaigns attempt to deliver the Dridex banking Trojan via malicious email attachments. Dridex is going through another ‘development phase’ which includes the abuse of devices known as Private Branch Exchange (PBX).

These devices ship with default credentials. It is likely that Secure Shell (SSH) is being used to administer the devices leveraging the default credentials and subsequently proxying some of the malicious activity.



The following is a reminder of the persistent threat Dridex poses to businesses. Fujitsu CTI provides updates & intelligence where appropriate on the capabilities the botnet gains.

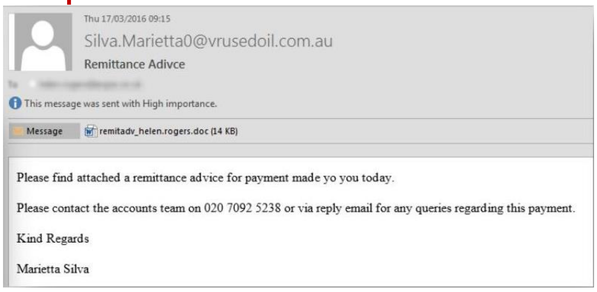
Threat

The victim will receive a well-engineered email with appropriate signature imagery which appears legitimate. Attachments are usually a Microsoft Word or Excel document which depending on security settings may prompt you to ‘Enable content’ and in some cases includes instructions on how to enable Macros.

Example Senders & subject lines

- Sender: bounce@interparcel.com Subject: Interparcel Documents
- Sender Booth. Garth19@idsbangladesh.net.bd Subject: Remittance Advice

Example Email



Thu 17/03/2016 09:15
Silva.Marietta0@vrusedoil.com.au
Remittance Adivce

This message was sent with High importance.

Message | remitadv_helen.rogers.doc (14 KB)

Please find attached a remittance advice for payment made yo you today.

Please contact the accounts team on 020 7092 5238 or via reply email for any queries regarding this payment.

Kind Regards

Marietta Silva

Detection and remediation

Fujitsu CTI (FCTI) is proactively identifying the malicious addresses used in defined stages of the campaign in an effort to mitigate this threat. Additionally FCTI actively submit abuse notifications to ISP’s and liaises with European CERT agencies and law enforcement.

It is recommended Microsoft patches are applied regularly as per the best practices associated with CPNI and practice caution when opening attachments from unknown, or even known, senders.

Further Reading:
http://www.cpni.gov.uk/advice/cyber/spear-phishing/
http://blog.avira.com/dridex-starts-hardening-settings-files/

For more information, please contact:
Fujitsu Managed Security Services
fapl.askMSS@sg.fujitsu.com