SOC Threat Advisory - Threat Level - WARNING
Dridex development

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 malicous payload
21/10/2016

Synopsis

Fujitsu CTI have been monitoring Dridex across our customers for a period of time. There have been evolving variants of the same campaigns attempting to deliver the Dridex banking Trojan via malicious email attachments, Dridex has again undergone a development phase as it attempts to steal more sensitive material associated with banking assets.

The recent change affects the delivery mechanism which has moved from a prompt to, 'Enable Macros' to an embedded object inside the document which, if enabled would execute a script and download the malware. This particular sample was observed targeting Switzerland.

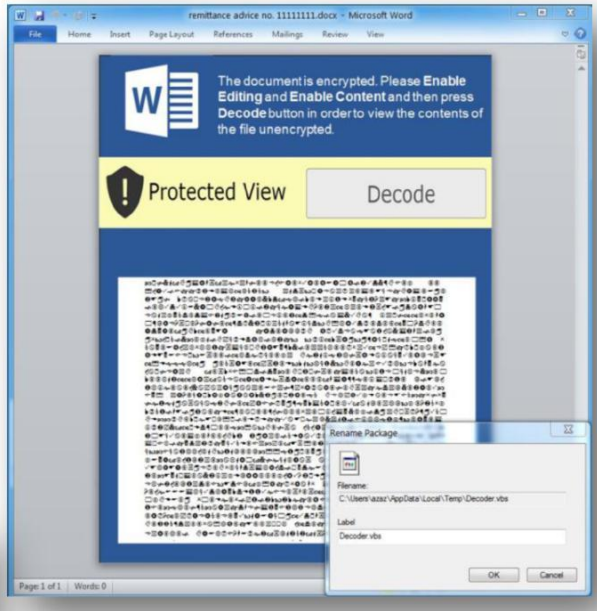
Further additions in this campaign include the use of WMI & PowerShell to execute commands locally.

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

Threat

The victim will receive a well-engineered email with appropriate signature imagery and appears legitimate. Attachments evolved from Word & Excel to JavaScript attachments which depending on security settings may prompt you to, 'Enable content' and in some cases include instructions on how to enable Macros.

Sample Malicious document



The SOC are proactively identifying the malicious addresses used in defined stages of the campaign in an effort to mitigate this threat, additionally the SOC actively submit abuse notifications to ISP's and liaises with law enforcement, and the NCSC.

It is recommended Microsoft patches are applied regularly as Per the best practises associated with CPNI and exercise caution when opening attachments from unknown senders

Further Reading

http://www.cpni.gov.uk/advice/cyber/spear-phishing/

http://www.symantec.com/content/en/us/enterprise/media/secu rity_response/whitepapers/dridex-financial-trojan.pdf

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