National Cyber Security Centre
a part of GCHQ

Advisory: Trickbot banking trojan

Busy reader's guide

28 September 2018

© Crown Copyright 2018

Introduction

The Trickbot banking trojan is being used in cyber attacks against small and medium-sized businesses, and individuals in the UK and overseas.

Trickbot attacks are designed to access online accounts, including bank accounts, with the goal of obtaining Personally Identifiable Information (PII) which can be used to facilitate identity fraud.

Trickbot continues to exploit trusted commercial and government brands using well-crafted phishing emails to initiate an infection.

This report details mitigations that organisations and individuals should implement immediately.

What Trickbot does

Trickbot is reported to have a range of malicious capabilities, including the ability to:

- Steal sensitive information, including banking login details and memorable information, by manipulating web-browsing sessions
- Gather detailed information about infected devices and networks
- Steal saved online account passwords, cookies and web history
- Steal login credentials for infected devices
- Connect infected devices to malicious, criminally controlled, networks over the Internet
- Spread by infecting other devices on the victim's network
- Download further malicious files such as Remote Access Tools, VNC clients, or ransomware

Protective action to take now

• Run a full scan on all devices using up to date antivirus / anti-malware software, such as Windows Defender. This should detect and remove any Trickbot infection.

See the *Mitigation* section below for further advice

Dealing with a possible Trickbot infection

Victims of Trickbot have observed a number of malicious actions following infection, including unauthorised access attempts to online accounts and successful, fraudulent bank transfer activity.

Several victims have also seen the infection spread to other networked machines, as well as noting changes to their network infrastructure.

To protect business and personal banking facilities, including where employees have accessed personal banking from work devices:

- Consider changing passwords and memorable information for any corporate, business or personal internet banking facilities (or other online resources) accessed from the infected network
- Review bank and credit card statements for suspicious activity and report any findings to your bank. Advise any employees who have accessed online banking facilities from the affected network to do likewise
- If you (or your employees) have been the victim of fraud, report it to Action Fraud

Mitigation:

Protect your devices and networks by keeping them up to date

- Use the latest supported versions, apply security patches promptly, use antivirus and scan regularly to guard against known malware threats. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/mitigating-malware.

Prevent and detect lateral movement in your enterprise networks

- See NCSC Guidance: https://www.ncsc.gov.uk/guidance/preventing-lateral-movement.

Implement architectural controls for network segregation

- This would help mitigate the exposure of the SMB issues described in the report. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/10-steps-network-security.

Set up a security monitoring capability

- This will enable you to collect the data that will be needed to analyse network intrusions. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/10-steps-monitoring and https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes.

Whitelist applications.

- If supported by your operating environment, consider whitelisting permitted applications. This will help prevent malicious applications from running. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/eud-security-guidance-windows-10-1709.

Use antivirus

- Keep any antivirus software up to date, and consider use of a cloud-backed antivirus product that can benefit from the improved threat intelligence and more advanced analysis which large scale operations bring. Ensure that it is also capable of scanning MS Office macros. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/macro-security-microsoft-office.

Use Multi-Factor Authentication (MFA)

Mitigate against password guessing and theft, including brute force attacks by using MFA. MFA can also be called two-step verification or 2-factor authentication (2FA). See NCSC Guidance: https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services.