UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00107

AGENT TESLA RAT DISABLES MICROSOFT ASMI

DATE ISSUED: 15th February 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

A new version of the Remote Access Trojan (RAT) 'Agent Tesla' has been discovered which has the ability to immobilise Microsoft's Anti-Malware Software Interface (ASMI) in an effort to evade detection.

BREAKDOWN

The ASMI in Microsoft Windows allows the operating system to integrate with anti-malware software provided by security vendors so by targeting this function, the Agent Tesla malware is able to avoid detection. Further measures to conceal its communications are taken by deploying a Tor client and utilising Telegram chat application to covertly exfiltrate data. Agent Tesla is fast becoming one of the top malware families, as detected in malicious attachments by Sophos, and is likely to be continually upgraded and modified to evade detection and add complexity for reverse engineering. Initially specialising in key-logging, this malware has evolved significantly since its first detection in 2014 and historically is known to be propagated through malicious emails and SPAM. Agent Tesla targets the ASMI by locating the address of the AmsciScanBuffer and patches the first 8bytes of the function to it's own memory causing AMSI scans to be seen as invalid and skipping over further scans in the first stage of its execution. This step prevents detection for the second stage loader containing the payload. This new version includes functions to capture the contents of the clipboard and search for credentials to be harvested from web browsers and email clients as well as browser cookies which are then exfiltrated to the Command and Control (C2) centre. These features are though to be premium features that must be purchase from the malware's developer.

REMEDIATION STEPS

- Use anti-malware detection and remediation software on all endpoint devices.
- Monitor network activity for any suspicious or anomalous behaviour.
- Educate users on the dangers of malicious emails, how to spot them, what to do with them and where to report them. Use phishing simulation exercises to assist with user awareness training.
- Use Secure Email Gateway and SPAM filters to prevent suspicious emails from reaching users.

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/agent-tesla-microsoft-asmi/163581/
The Cyber Security News https://thecybersecurity.news/vulnerabilities/agent-tesla-trojan-kneecaps-microsofts-anti-malware-interface-5797/