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

CYBER GUIDANCE ISSUE 00234

RATDISPENSER DOWNLOADS TROJANS & OTHER MALWARE

DATE ISSUED: 14th December 2021

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

A new javaScript downloader is on the scene and is being used to distribute 8 different types of Remote Access Trojans (RATs) and other information stealing malware and key loggers to steal credentials or other sensitive data and establish a backdoor for attackers into Windows systems.

BREAKDOWN

Researchers at HP Wolf Security have dubbed this new threat RATDispenser, which is being distributed by phishing emails claiming to contain details about a product order in a text file. The attachment contains the malware and kicks off the execution, which avoids detection using long strings of code to obscure its malicious intent. After installation, the malware is used to distribute a variety of malware to steal information. The malware was only detected by 1 in 10 anti-virus engines when tested. The two malware downloads that proved most popular were STRRT and WSHRAT, and others were Adwind, Formbook, Remcos, Panda Stealer, GuLoader and Ratty.

REMEDIATION STEPS

- Educate users on the dangers of social engineering and how to detect phishing emails, as well as what to do with any suspicious emails in your organisation.
- System administrators should audit file types allowed the reach end users through their email gateway (such as executables) and set up rules preventing users from running any executable files.

REFERENCES & RESOURCES

ZDNet https://www.zdnet.com/article/this-stealthy-malware-delivers-a-silent-threat-that-wants-to-steal-your-passwords/

HP Threat Research https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild/

Bleeping Computer https://www.bleepingcomputer.com/news/security/stealthy-new-javascript-malware-infects-windows-pcs-with-rats/