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

CYBER GUIDANCE ISSUE 00226

MICROP RANSOMWARE SPREAD VIA GOOGLE DRIVE

DATE ISSUED: 23rd November 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

By using legitimate cloud services like Google Drive to host malicious pages and content, attackers are circumventing Secure Email Gateway (SEG) protections to distribute a Halloween-themed malware – MICROP.

BREAKDOWN

Distributed by phishing emails, the original campaign feature a link to a Google Drive URL asking for support for a "DWG following Supplies List" which when accessed by a user downloads a .MHT file. Users who open the file see a blurred out, stamped form while the .MHT file in the background is downloading a .RAR file containing the executable malware DotNETLoader. This then uses a VBS script to run the ransomware in memory, which is known as both MICROP and Crypt888. Once the victim's machine is encrypted, instructions are displayed in the form of a gruesome wallpaper and they will only able to access a web browser to contact the attacker by email and arrange payment – all other files and applications are locked down. Once payment is successfully made, the attacker provides a decryption tool to their victim. Not only does this malware encrypt files on the targeted machine, but it also steals passwords from web browsers such as Chrome, Firefox, Explorer and Opera. By using the legitimate Google Drive service, phishing emails are able to sneak past SEG and other protection mechanisms.

REMEDIATION STEPS

- Educate users on social engineering and phishing emails – how to detect them and what to do with any emails they deem suspicious received within your organisation.
- Implement a Next Generation Secure Email Gateway to assist with detecting malicious email activity, both inbound and outbound that also features time-of-click protection which prevents users accessing known malicious links in emails.
- Run Endpoint Protection (NGAV) on all devices to detect and respond to unusual behaviours.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/ransomware-phishing-emails-segs/176470/
Trend Micro https://blog.trendmicro.com/6-scariest-faces-ransomware/