U UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00110

SILVER SPARROW AWAITS ON MAC CHIPSETS

DATE ISSUED: 22nd February 2021

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

Apple’s new M1 chip has become the target of Silver Sparrow novel malware which appears to be lying in wait for further instructions after infection thousands of Mac devices.

BREAKDOWN

Red Canary analysts have discovered the latest strain of malware executing on the in-house Apple chipset however, the final payload or intention hasn’t made itself known yet. The malware seems to be awaiting further instruction indicating the sophistication of the attackers and their forward-thinking planning and has been found on 29.139 devices worldwide thus far. The construction and execution methods of this malware creates abundant opportunities for development and improvement in the future. Further discoveries suggest this may be an adware that targets both Intel and M1-based devices by using a JavaScript execution and it is unknown as to how the malware is being distributed. The malware has been traced back to an Amazon Web Service S3 cloud platform with callback domains hosted through Akamai’s CDN (content delivery network) which are both commonly used by many organisations so would be difficult to blacklist or block these services.

REMEDIATION STEPS

- See Indicators of Compromise (IoC),and remediations suggested by Red Canary for both version of the malware in the references below.
- Use compatible anti-malware software to conduct scanning of your Apple devices and take action on any suggested remediations.

REFERENCES & RESOURCES

Red Canary	https://redcanary.com/blog/clipping-silver-sparrows-wings/
Threatpost	https://threatpost.com/silver-sparrow-malware-30k-macs/164121/