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

CYBER GUIDANCE ISSUE 00116

ATTACKERS USE SEO TO DEPLOY MALWARE

DATE ISSUED: 8th March 2021

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

OVERVIEW

By abusing Search Engine Optimisation (SEO), attackers are ramping up website positioning in internet search engines, such as Google, as a method to deploy malware through compromised websites.

BREAKDOWN

The abuse of SEO allows attackers to legitimately boost the ranking and exposure of their website, making them appear high on the list of returned search results. A highly sophisticated version of this attack has been discovered by Sophos Labs, which they have named "GootLoader" due to the association with the Gootkit Remote Access Trojan (RAT), with the attacks believed to be carried out by over 400 servers. Other malware may also be dropped by this particular kit including REvil, Kronos and Cobalt Strike. An attacker must first compromise a website and inject a few lines of code into the body content, thereafter the websites are manipulated so that when certain terms are searched, under the right conditions – based on their level of interest to the attacker based on IP address and location and where the search query originated from, the information presented to the victim is rewritten to certain visitors. It will appear to the victim as the discovery of a new forum or blog comment section relating to their searched topic with an answer to the original query with a clickable link. At this point a zip archive file is downloaded with the searched term as the name containing an .js executable file which contains the malware. If the conditions are not me the website will appear normal at first but eventually dissolve.

REMEDIATION STEPS

- Use script blockers while surfing the web such as NoScript for Firefox.
- Check for a certificate or https (padlock in the address bar) when browsing the web.
- Refrain from clicking links unless you are 100% sure of where they lead.
- Never open zipped files from new or unusual website.
- Educate users on the dangers of social engineering and various types of attacks.

REFERENCES & RESOURCES

ZDNet https://www.zdnet.com/article/hackers-exploit-websites-to-give-them-excellent-seo-before-deploying-malware/
Heimdal Security https://heimdalsecurity.com/blog/seo-techniques-used-for-malware/
Threatpost https://threatpost.com/malware-loader-google-seo-payload/164377/