A Current Cybersecurity Attack: Using GootLoader

I came across a very interesting article entitled “New GootLoader Campaign Targets Users Searching for Bengal Cat Laws in Australia” (Lakshmanan, 2024b). The name GootLoader caught my attention and the peculiarity of Bengal cat laws got me to click on it. The name GootLoader has two parts ‘Goot’ and ‘Loader’. The ‘Loader’ part means that it is a malware loader. Meaning that when victims download and run this file, it will load or download other malware onto their system. ‘Goot’ refers to GootKit which is loaded onto systems by GootLoader and is a trojan that focuses on stealing banking credentials.

The other part of the title that intrigued me was targeting people searching for Bengal cat laws in Australia. When people used a search engine looking for information on the Australian laws on Bengal cats, one of the top results would be a malicious website. The bad actors spreading the GootLoader utilized search engine optimization (SEO) poisoning. SEO is a practice where a website will optimize what appears on their site to bring their result closer to the top on popular search engines. SEO poisoning is simply the use of SEO on a malicious website. Part of the reason the bad actors chose Bengal cat laws in Australia is that there would be fewer other websites with that information, making their SEO job easier. Another is that the GootLoader would have to download itself, so they used the guise of legal documents or agreements to justify the download to unsuspecting users.

The malicious website would automatically download a .zip file into the user’s downloads folder. The .zip file was named “Are_bengal_cats_legal_in_australia_[5 digit number].zip” (Tang et al., 2024) and contained a JavaScript file with a similar name. When that JavaScript file is executed, it downloads a larger JavaScript file named “Small Units Tactics.js” which was obfuscated, meaning it was difficult to read and understand. The initial JavaScript file also created a file named “Huthwaite SPIN selling.dat” and a Scheduled Task with a random name like “Destination Branding”. The Schedule Task was used WScript.exe and the locations of the files were in a Windows format, so this malware would only work properly on Microsoft Windows.

Then cscript.exe would be run, which is another Windows tool, to then run a PowerShell.exe instance. The cscript.exe establishes persistence, meaning that the bad actors won’t lose access to the system, using the Scheduled Task. The PowerShell instance would send requests to various domains along with base-64 encoded cookies containing system information and some directory paths the bad actors were looking for. It would also download and execute any other malware on those domains, so the bad actors could continue with whatever they want.

To recap, someone searches for Australian Bengal cat law in any search engine. They click on the malicious website which automatically downloads the GootLoader as a .zip file with the name closely matching their search. The user unzips the archive and executes a JavaScript file of the same name as the .zip archive. Then without their

knowledge a series of actions occur like the creation of files, fetching of more files, and creation of a Scheduled Task. And now the user's computer is infected with whatever malware the bad actors wish and system information is sent to them as well. The GootLoader only works properly on Microsoft Windows as it uses Windows specific tools and path formatting.

Of course, the group behind this isn't limiting themselves to the, probably very few, people that search for Bengal cat laws in Australia. The GootKit malware has been around for a decade at this time. Around 2020, researchers saw a surge in GootLoader instances targeting users in Germany, the U.S., France, and South Korea. Researchers even found that some of the sites would change to hide the malware for visitors outside of regions the bad actors were targeting. The group behind it have also been improving GootLoader over time with 3 different versions currently in use. The way that GootLoader works has remained about the same, but the malware brought in by the PowerShell script changes. Some other than GootKit have been IcedID, SystemBC, Cobalt Strike, REvil, and Kronos (Lakshmanan, 2024a). One of the different versions of GootLoader, called GootBot, adds capabilities for lateral movement and does a better job evading detection measures. Making it even more dangerous as it allows the attackers to get infected machines to try and spread GootBot as well as hiding more effectively.

In November 2024, a security researcher stopped finding samples of GootLoader from regional law searches. Instead, the samples were named like "[Last Name] Resume 2024" or "Dr. [Last Name] request form" and were found using a Yara rule. But the researcher couldn't find them by manually searching so they reached out for help. Someone returned to the researcher with an advertisement for a "PDF to DOCX converter." Users would upload their desired .pdf file and would get a .zip archive containing the .docx file, but if you were from an English-speaking country and weren't visiting from the same IP in 24 hours you would get a JavaScript file in the .zip archive. The researcher speculates that the legal term SEO sites were targeted at corporations and the new .pdf to .docx sites might be a pivot to targeting home users.

Today's Internet is plagued with things to watch out for that are constantly evolving and not enough people can keep up. Even those that do keep up still fall for scams or malware on occasion when they aren't paying absolute full attention. Though this attack has a couple big red flags like the unsolicited download and a JavaScript file, there will inevitably be victims. The GootLoader is very dangerous because it allows the attacker to customize what happens next after the infection. The use of search engine optimization poisoning also enables the attacker to target specific groups to make their campaign more effective. The evolving nature and random words/numbers in the GootLoader malware makes is difficult to detect and eliminate. These culminating factors make for a malware that will cost many people a lot of money.

Gootloader's Pivot from SEO Poisoning: PDF Converters Become the New Infection Vector. (2024, November 7). Gootloader Details. https://gootloader.wordpress.com/2024/11/07/gootloaders-pivot-from-seo-poisoning-pdf-converters-become-the-new-infection-vector/

Lakshmanan, R. (2021, March). *Gootkit RAT Using SEO to Distribute Malware Through Compromised Sites*. The Hacker News. https://thehackernews.com/2021/03/gootkit-rat-using-seo-to-distribute.html

Lakshmanan, R. (2023, November 7). *New GootLoader Malware Variant Evades Detection and Spreads Rapidly*. The Hacker News. https://thehackernews.com/2023/11/new-gootloader-malware-variant-evades.html

Lakshmanan, R. (2024a, July 5). *GootLoader Malware Still Active, Deploys New Versions for Enhanced Attacks*. The Hacker News. https://thehackernews.com/2024/07/gootloader-malware-delivers-new.html

Lakshmanan, R. (2024b, November 11). *New GootLoader Campaign Targets Users Searching for Bengal Cat Laws in Australia*. The Hacker News. https://thehackernews.com/2024/11/new-gootloader-campaign-targets-users.html

Tang, T., Koike, H., Castle, A., & Gallagher, S. (2024, November 6). *Bengal cat lovers in Australia get psspsspss'd in Google-driven Gootloader campaign*. Sophos News. https://news.sophos.com/en-us/2024/11/06/bengal-cat-lovers-in-australia-get-psspsspssd-in-google-driven-gootloader-campaign/