Trend Research

TREND MICRO

The Rise of Residential Proxies and Its Impact on Cyber Risk Exposure Management

Appendix

Appendix Note

This appendix further discusses bulletproof hosting and how it enables cybercrime. It also discusses residential proxies and the different ways they are provisioned.

Bulletproof Hosting (BPH)

Bulletproof hosting (BPH) refers to hosting services that facilitate malicious and criminal activities by allowing content and operations typically not allowed by legitimate hosting providers[1]. It is also known as abuse-resistant hosting services. These services offer internet infrastructure for Command and Control (C&C) servers, the storage of restricted and stolen content, and other criminal activities such as malware creation, distribution, and operation.

The effectiveness of bulletproof hosting lies in the reseller's ability to match customer demands and manage relationships with legitimate hosting providers and upstream providers to handle abuse requests.

Bulletproof hosting providers often ignore abuse requests and alert their customers in advance, allowing for time to adjust operations. They also offer features that can help cybercriminals conceal their identities from investigators.

Some bulletproof hosts use stolen or compromised assets, but these assets can be cleaned up when abuse gets detected by the original owners, so they are often used for short-lived activities like spam distribution.

Meanwhile, other bulletproof hosting providers rent servers from multiple resellers of legitimate webhosting providers, thus creating the risk of being terminated by the legitimate webhosting providers. Another type of bullet proof hosting provider has their own Autonomous System Number (ASN) and gets their internet connectivity from one or more upstream providers, which makes a takedown even harder. While some providers own their hardware, many BPH providers operate as marketplaces, reselling hosting services from other providers.

Provisioning residential proxies

Residential proxies are provisioned through various methods. A lot of the residential proxies are installed on devices with the users' consent, although it can be assumed that most of those users do not understand the full extent and risk of allowing their device to be added to a residential proxy network. Other residential proxies are part of a malware botnet, and some are the result of a supply chain compromise. In this part of the appendix, we discuss several methods how residential proxies are provisioned.

Residential proxies based on SDK

A common method of provisioning residential proxies is through Software Development Kits (SDK). This technique is widely used in both mobile applications and desktop applications. A proxy component is embedded in an SDK that gets installed along with the actual application the end user is interested in. Residential proxy companies are known to pay developers for bundling their SDK into "free" software or shareware. The SDK would provide a lengthy end-user license agreement (EULA) that basically says that the user agrees that the software routes network connections through the user's system to access public Internet resources. Since the EULA is lengthy and filled with legal terms, users are likely to click on "Agree" without knowing what exactly they are agreeing to.

Residential proxies and compromised network devices

Some residential proxy providers build their node pools by exploiting edge and network devices such as routers, IP cameras, and other IoT devices that are exposed to the internet. In an example, the compromised IoT devices of Water Barghest were made available for rent on a residential proxy service within minutes after initial infection[2].

Residential proxies and social engineering

Some residential proxy services source their exit nodes from software providers that trick users into downloading and installing extra software. For example, a user might want to download a shareware and involuntarily click on "Install bundled toolbox" or a similar prompt. The author of the shareware might hence obtain some incentives by sharing its users' computing or network resources[3].

Residential proxies provisioned through pre-infected IoT devices and phones

Some residential proxies get sourced from pre-infected devices. These devices may not be infected by their manufacturer, but the firmware installed on them is preloaded with malicious code. This compromise can occur at any stage during the firmware supply chain. It is important to understand that the pre-infected devices communicate with a C&C that has the capability to load additional modules onto the devices.

These modules belong to the monetization strategies of the threat actor; residential proxies are one of the core monetization strategies, but it is not the only strategy we have observed. In our research we have found other modules that are designed for specific tasks: such as automating account creation, receiving SMS message for authentication codes and one-time passwords, SMS spamming, and harvesting authentication credentials. There are also modules used as a fake search engine.

A leaked backend system that was used by Lemon group[4] revealed that pre-infected Android devices could be instructed to download and install specific modules. Over the years, the Lemon group developed many modules such as proxy and SMS landing components. The plugAD.zip module as illustrated in Figure 1 was designed to manipulate advertisements on social media.

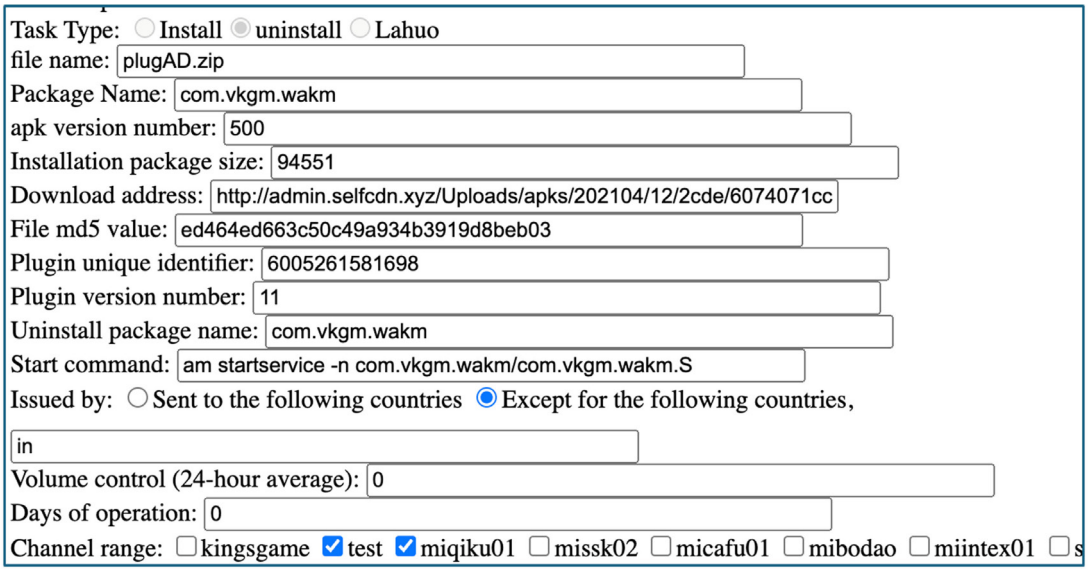

Figure 1. The backend system of Lemon group that can install specific malicious modules on pre-infected Android devices

The Lemon Group is not the only actor group who deploys pre-infected Android applications and uses a modular model that allows for the installation of specific malicious components on endpoints. Other cybercriminals are using the same model, and this model can potentially make detection of residential proxies even harder.

The type of residential proxy service provider that sources their exit nodes from pre-infected IoT devices and phones usually sells both residential and mobile proxies. The main reason is that the backdoored devices may sometimes be connected to a Wi-Fi network, while in other cases it may be connected to a cellular network.

Non-residential proxies

There are many other online services that offer proxies for rent. Instead of residential proxies, they rent out data center IP addresses. These proxy services are procured through renting hosts at bullet proof hosting providers and are layered with redundant and resistant architecture.

References

1 https://documents.trendmicro.com/assets/white_papers/wp-the-hacker-infrastructure-and-underground-hosting-cybercrime-modi-operandi-and-opsec.pdf

2 https://www.trendmicro.com/en_nl/research/24/k/water-barghest.html

3 https://www.trendmicro.com/en_us/research/23/b/hijacking-your-bandwidth-how-proxyware-apps-open-you-up-to-risk.html

4 https://www.trendmicro.com/en_nl/research/23/e/lemon-group-cybercriminal-businesses-built-on-preinfected-devices.html