Thieves Reaching for Linux—”Hand of Thief” Trojan Targets Linux #INTH3WILD

web.archive.org/web/20130815040638/https://blogs.rsa.com/thieves-reaching-for-linux-hand-of-thief-trojan-targets-linux-inth3wild/

August 7, 2013

Just two weeks after reporting about the commercialization of the KINS banking Trojan, RSA reveals yet another weapon to be used in a cybercriminal’s arsenal.

It appears that a Russia based cybercrime team has set its sights on offering a new banking Trojan targeting the Linux operating system. This appears to be a commercial operation, which includes support/sales agents and software developer(s).

Meet the “*Hand of Thief*” Trojan

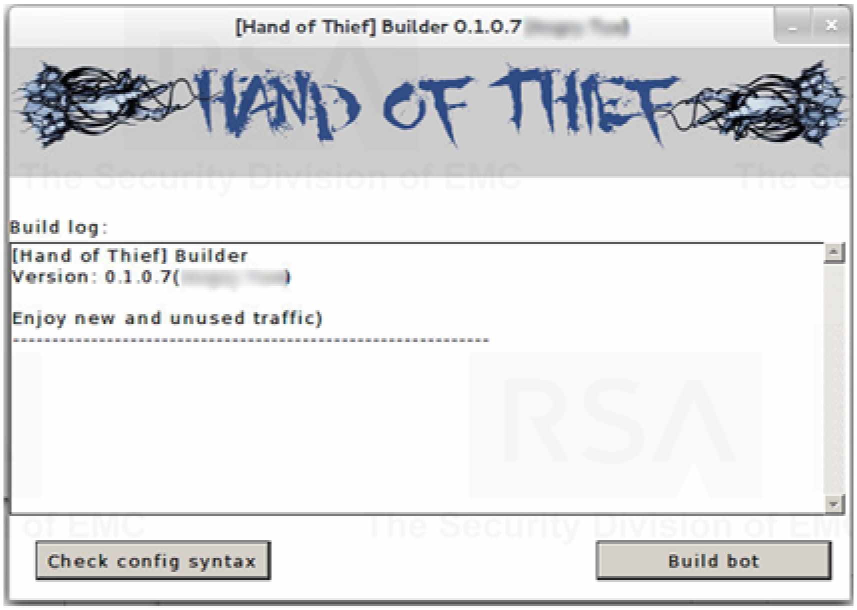
Hand of Thief is a Trojan designed to steal information from machines running the Linux OS. This malware is currently offered for sale in closed cybercrime communities for $2,000 USD (€1,500 EUR) with free updates. The current functionality includes form grabbers and backdoor capabilities, however, it’s expected that the Trojan will have a new suite of web injections and graduate to become full-blown banking malware in the very near future. At that point, the price is expected to rise to $3,000 USD (€2,250 EUR), plus a hefty $550 per major version release. These prices coincide with those quoted by developers who released similar malware for the Windows OS, which would make *Hand of Thief* relatively priced way above market value considering the relatively small user base of Linux.

The Trojan’s developer claims it has been tested on 15 different Linux desktop distributions, including Ubuntu Fedora and Debian. As for desktop environments, the malware supports 8 different environments, including Gnome and Kde.

An Insider’s Glimpse

RSA researchers have managed to obtain the malware builder as well as the server side source code, and a preliminary analysis reveals familiar functionalities of a banking Trojan. Some of the initial features include:

- Form grabber for both HTTP and HTTPS sessions; supported browsers include Firefox, Google Chrome, as well as several other Linux-only browsers, such as Chromium, Aurora and Ice Weasel.
- Block list preventing access to specified hosts (*a similar deployment used by the Citadel Trojan to isolate bots from security updates and anti-virus providers*)
- Backdoor, backconnect and SOCKS5 proxy
- Anti-research tool box, which includes anti VM, anti-sandbox and anti-debugger



Build log:

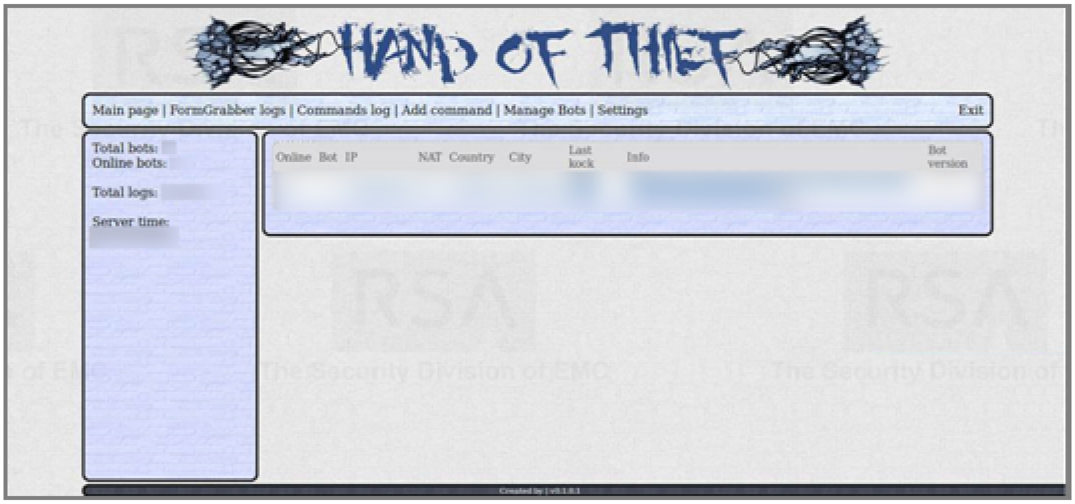
```
[Hand of Thief] Builder
Version: 0.1.0.7([redacted])

Enjoy new and unused traffic)
------------------------------------------------------------
```

Figure 1: Hand of Thief – Linux Trojan’s Builder

Control Panel Features

The developer wrote a basic administration panel for the Trojan, allowing the botmaster to control the infected machines reporting to it. The panel shows a list of the bots, provides a querying interface, and run of the mill bot management options.

The Trojan’s infrastructure collects the stolen credentials and stores the information in a MySQL database. Captured data includes information such as timestamp, user agent, website visited and POST data. *Hand of Thief* also exhibits cookie-stealing functionality.


HAND OF THIEF
Main page | FormGrabber logs | Commands log | Add command | Manage Bots | Settings
Exit

Total bots: [redacted]
Online bots: [redacted]

Total logs: [redacted]

Server time: [redacted]

Online	Bot	IP	NAT	Country	City	Last kock	Info	Bot version
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Figure 2: Hand of Thief – Linux Trojan’s Admin Panel View

Although *Hand of Thief* comes to the underground at a time when commercial Trojans are high in demand, writing malware for the Linux OS is uncommon, and for good reason. In comparison to Windows, Linux’s user base is smaller, considerably reducing the number of potential victims and thereby the potential fraud gains. Secondly, since Linux is open source, vulnerabilities are patched relatively quickly by the community of users. Backing this up is the fact that there aren't significant exploit packs targeting the platform. In fact, in a conversation with the malware's sales agent, he himself suggested using email and social engineering as the infection vector.

So What's Next?

We are left with a number of questions:

Without the ability to spread the malware as widely as on the Windows platform, the price tag seems hefty, and raises the question – will the Linux Trojan have the same value as its Windows counterparts?

Also, with recent recommendations to leave the supposedly insecure Windows OS for the safer Linux distributions, does *Hand of Thief* represent the early signs of Linux becoming less secure as cybercrime migrates to the platform?

Only time will tell. RSA researchers will continue to closely monitor the development of this Trojan and update accordingly.