400k Linux servers compromised for cryptotheft and financial gain

ESET RESEARCH

Ebury is alive but unseen: 400k Linux servers compromised for cryptocurrency theft and financial gain

One of the most advanced server-side malware campaigns is still growing, with hundreds of thousands of compromised servers, and it has diversified to include credit card and cryptocurrency theft

Marc-Etienne M.Léveillé

14 May 2024 , 3 min. read

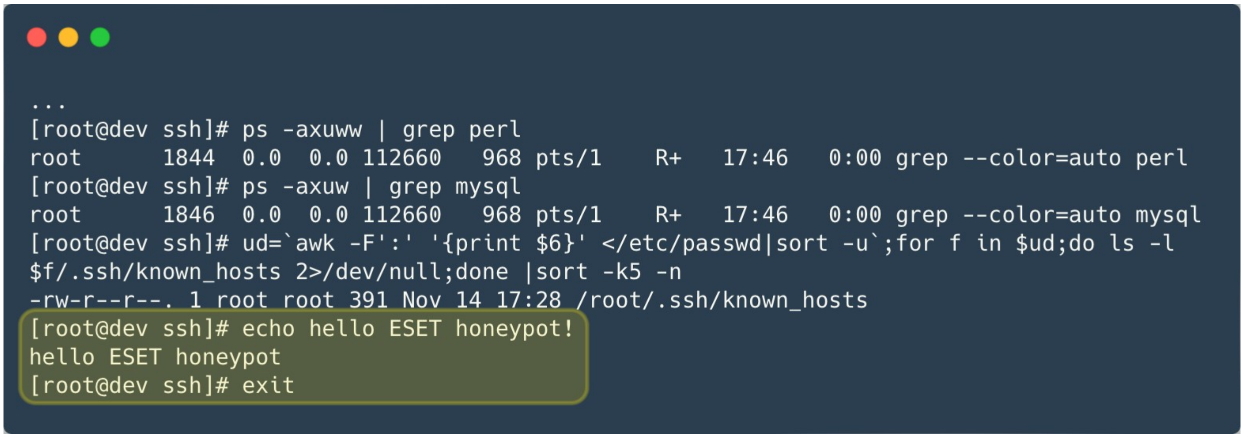
Ten years ago we raised awareness of Ebury by publishing a white paper we called Operation Windigo, which documented a campaign that leveraged Linux malware for financial gain. Today we publish a follow-up paper on how Ebury has evolved, and the new malware families its operators use to monetize their botnet of Linux servers.

Ebury is alive but unseen

Read full report

The arrest and conviction of one of the Ebury perpetrators following the Operation Windigo paper did not stop the botnet from expanding. Ebury, the OpenSSH backdoor and credential stealer, was still being updated, as we reported in 2014 and 2017.

We maintain honeypots to track new samples and network indicators. However, it has become more and more difficult to run such honeypots as Ebury evolved. For instance, one of our honeypots did not react exactly as expected when Ebury was installed. After spending hours trying to debug what was going on, Ebury operators finally abandoned the server and sent a message to show that they knew about our attempts at tricking them, as shown in Figure 1.



```
...
[root@dev ssh]# ps -axuww | grep perl
root      1844  0.0  0.0 112660   968 pts/1    R+   17:46   0:00 grep --color=auto perl
[root@dev ssh]# ps -axuw | grep mysql
root      1846  0.0  0.0 112660   968 pts/1    R+   17:46   0:00 grep --color=auto mysql
[root@dev ssh]# ud=`awk -F':' '{print $6}' </etc/passwd|sort -u`;for f in $ud;do ls -l
$f/.ssh/known_hosts 2>/dev/null;done |sort -k5 -n
-rw-r--r--. 1 root root 391 Nov 14 17:28 /root/.ssh/known_hosts
[root@dev ssh]# echo hello ESET honeypot!
hello ESET honeypot
[root@dev ssh]# exit
```

Figure 1. Interactions between the Ebury perpetrators and an ESET-operated honeypot, showing that the operators had flagged this system as a honeypot

In 2021, the Dutch National High Tech Crime Unit (NHTCU) reached out to ESET after they had found Ebury on the server of a victim of cryptocurrency theft. Working together, we gained great visibility into the recent activities of the group and the malware it uses.

Ebury, Ebury everywhere

This paper reveals new methods used to propagate Ebury to new servers. Figure 2 summarizes the methods we could document.

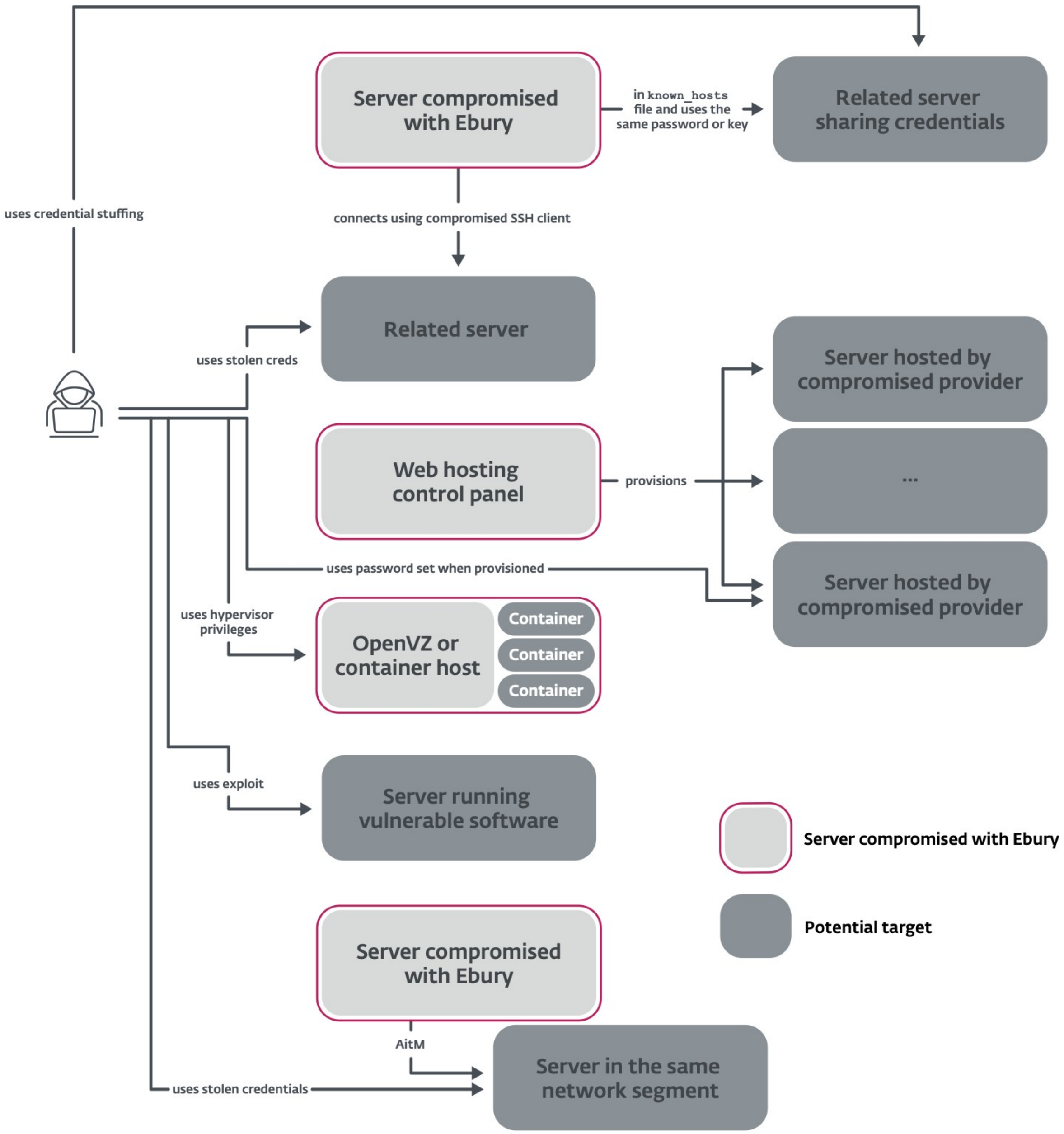

Server compromised with Ebury
in known_hosts file and uses the same password or key
Related server sharing credentials
uses credential stuffing
connects using compromised SSH client
Related server
uses stolen creds
Server hosted by compromised provider
Web hosting control panel
provisions
...
uses password set when provisioned
Server hosted by compromised provider
uses hypervisor privileges
OpenVZ or container host
Container
Container
Container
uses exploit
Server running vulnerable software
Server compromised with Ebury
Potential target
Server compromised with Ebury
AitM
uses stolen credentials
Server in the same network segment

Figure 2. Different methods used by the Ebury gang to compromise new servers

Among the victims are many hosting providers. The gang leverages its access to the hosting provider's infrastructure to install Ebury on all the servers that are being rented by that provider. As an experiment, we rented a virtual server from one of the compromised hosting providers: Ebury was installed on our server within seven days.

Another interesting method is the use of adversary in the middle to intercept SSH traffic of interesting targets inside data centers and redirect it to a server used to capture credentials, as summarized in Figure 3. Ebury operators leverage existing Ebury-compromised servers in the same network segment as their target to perform ARP spoofing. According to internet telemetry, more than 200 servers were targeted in 2023. Among the targets are Bitcoin and Ethereum nodes. Ebury automatically steals cryptocurrency wallets hosted on the targeted server once the victim types the password to log into it.

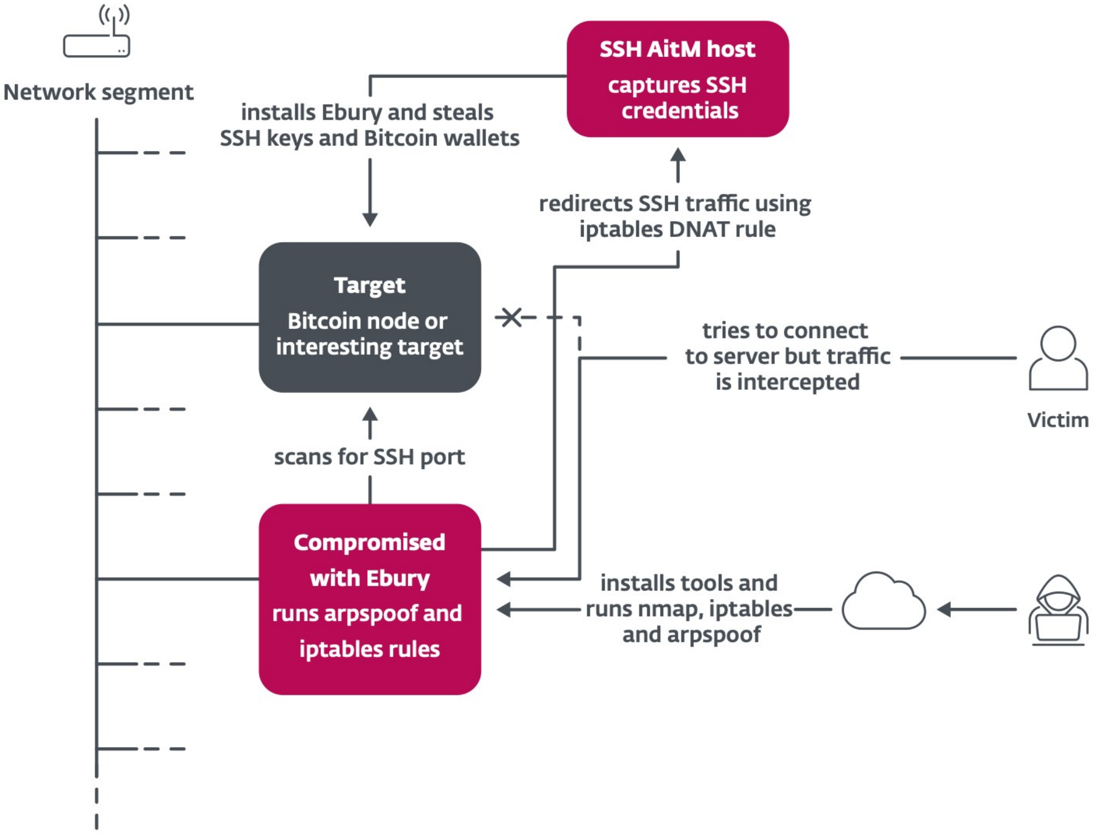

Network segment
SSH AitM host
captures SSH credentials
installs Ebury and steals SSH keys and Bitcoin wallets
redirects SSH traffic using iptables DNAT rule
Target
Bitcoin node or interesting target
tries to connect to server but traffic is intercepted
Victim
scans for SSH port
Compromised with Ebury
runs arpspoof and iptables rules
installs tools and runs nmap, iptables and arpspoof

Figure 3. Overview of AitM attacks perpetrated by the Ebury gang

So how effective are all these methods? Combined, about 400,000 servers have been compromised by Ebury since 2009, and more than 100,000 were still compromised as of late 2023. The perpetrators keep track of the systems they compromised, and we used that data to draw a timeline of the number of new servers added to the botnet each month (Figure 4). It is shown using two scales, to demonstrate some of the major incidents where Ebury was deployed on tens of thousands of servers at once.

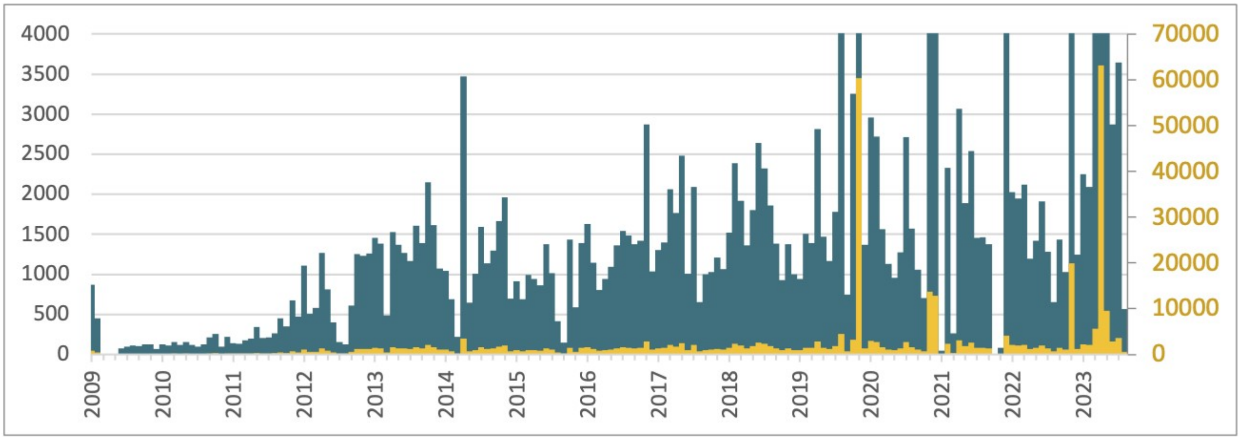


Figure 4. Ebury deployments per month using two different scales on the Y axis, according to the database of compromised servers maintained by the perpetrators

Monetization

This new paper uncovers new malware families used to leverage the Ebury botnet (Figure 5). In addition to spam and web traffic redirection that are still perpetrated by the gang, HTTP POST requests made to, and from, the servers are leveraged to steal financial details from transactional websites.

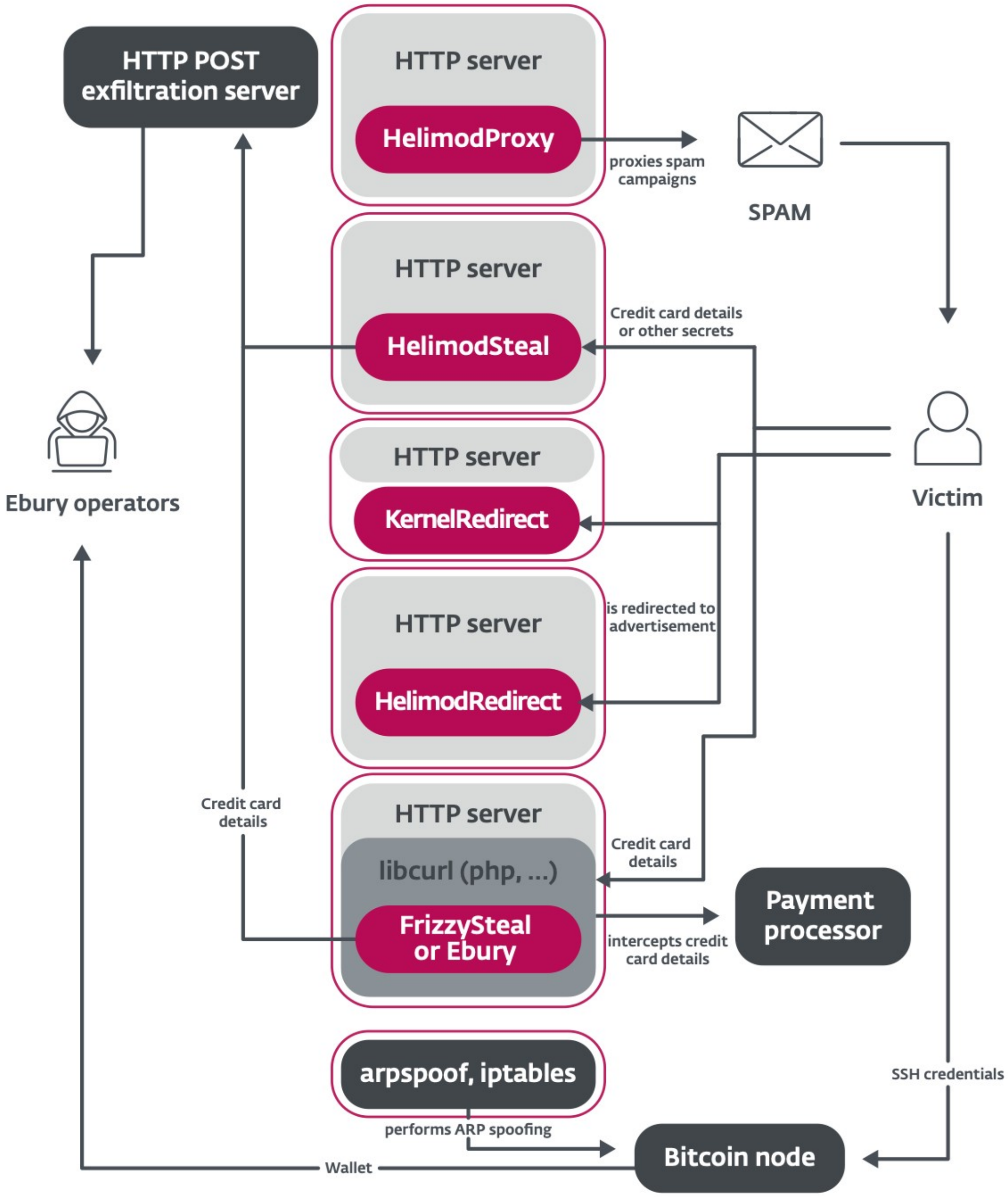
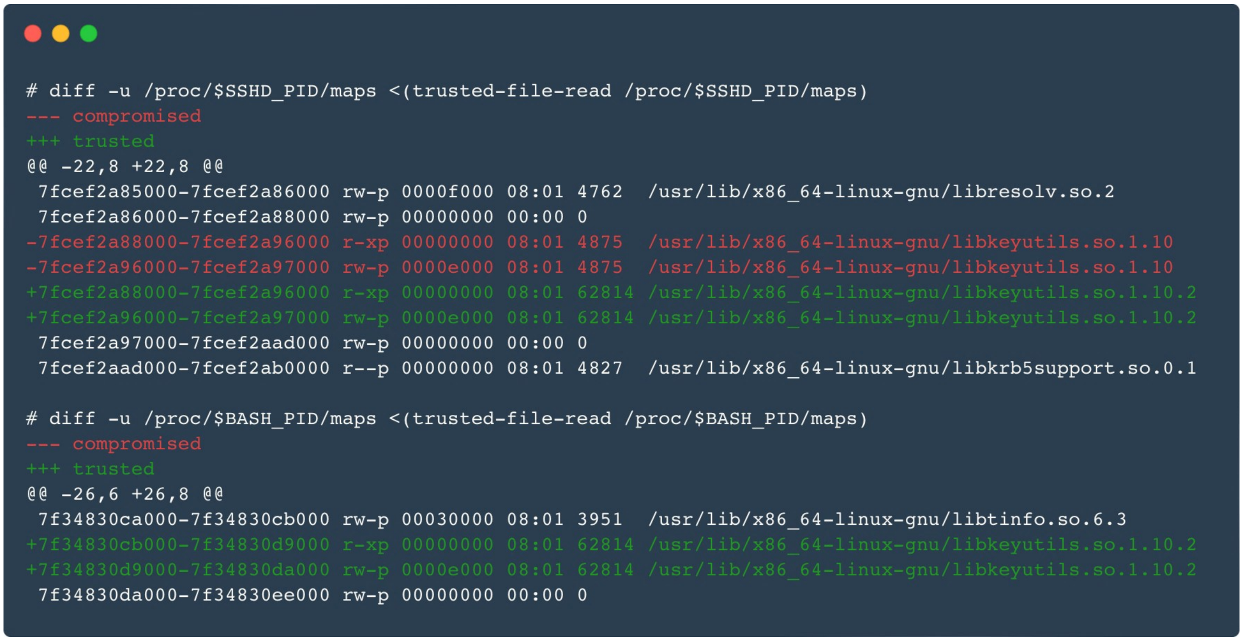


Figure 5. Multiple malware families deployed on Ebury-infested servers and the impact for potential victims

Hiding deeper

The Ebury malware family itself has also been updated. The new major version update, 1.8, was first seen in late 2023. Among the updates are new obfuscation techniques, a new domain generation algorithm (DGA), and improvements in the userland rootkit used by Ebury to hide itself from system administrators. When active, the process, the file, the socket, and even the mapped memory (Figure 6) are hidden.



```
# diff -u /proc/$SSHD_PID/maps <(trusted-file-read /proc/$SSHD_PID/maps)
--- compromised
+++ trusted
@@ -22,8 +22,8 @@
 7fcef2a85000-7fcef2a86000 rw-p 0000f000 08:01 4762  /usr/lib/x86_64-linux-gnu/libresolv.so.2
 7fcef2a86000-7fcef2a88000 rw-p 00000000 00:00 0
-7fcef2a88000-7fcef2a96000 r-xp 00000000 08:01 4875  /usr/lib/x86_64-linux-gnu/libkeyutils.so.1.10
-7fcef2a96000-7fcef2a97000 rw-p 0000e000 08:01 4875  /usr/lib/x86_64-linux-gnu/libkeyutils.so.1.10
+7fcef2a88000-7fcef2a96000 r-xp 00000000 08:01 62814 /usr/lib/x86_64-linux-gnu/libkeyutils.so.1.10.2
+7fcef2a96000-7fcef2a97000 rw-p 0000e000 08:01 62814 /usr/lib/x86_64-linux-gnu/libkeyutils.so.1.10.2
 7fcef2a97000-7fcef2aad000 rw-p 00000000 00:00 0
 7fcef2aad000-7fcef2ab0000 r--p 00000000 08:01 4827  /usr/lib/x86_64-linux-gnu/libkrb5support.so.0.1

# diff -u /proc/$BASH_PID/maps <(trusted-file-read /proc/$BASH_PID/maps)
--- compromised
+++ trusted
@@ -26,6 +26,8 @@
 7f34830ca000-7f34830cb000 rw-p 00030000 08:01 3951  /usr/lib/x86_64-linux-gnu/libtinfo.so.6.3
+7f34830cb000-7f34830d9000 r-xp 00000000 08:01 62814 /usr/lib/x86_64-linux-gnu/libkeyutils.so.1.10.2
+7f34830d9000-7f34830da000 rw-p 0000e000 08:01 62814 /usr/lib/x86_64-linux-gnu/libkeyutils.so.1.10.2
 7f34830da000-7f34830ee000 rw-p 00000000 00:00 0
```

Figure 6. Differences (in unified format) in OpenSSH server and Bash maps files when under the Ebury userland rootkit

Want to know more? Am I compromised?

The new paper, Ebury is alive but unseen: 400k Linux servers compromised for cryptocurrency theft and financial gain, goes into more details about each of Ebury's aspects, including many technical specifics.

Indicators of compromise are also available in ESET's malware-ioc GitHub repository, and a detection script is in the malware-research repository.

> *For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com*
> *ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page.*

Let us keep you up to date

Sign up for our newsletters