OPERATION WINDIGO

The vivisection of a large Linux server-side credential stealing malware campaign

Oh Sieng Chye, Researcher
ESET ASIA (Singapore)
Olivier Bilodeau • Pierre-Marc Bureau • Joan Calvet
Alexis Dorais-Joncas • Marc-Étienne M.Léveillé
Benjamin Vanheuverzwijn
Partners Acknowledgement

- Catherine Goerner-Potvin (artwork)
- The European Organization for Nuclear Research (CERN)
- CERT-Bund
- Emerging Threats
- Sucuri
- The Swedish National Infrastructure for Computing
- Valérie Motard (artwork adaptation)

- abuse.ch
- Spamhaus
- Maven Hosting
- PlusServer AG
ESET research team published a paper titled "Operation Windigo", detailing how thousands of Linux and Unix servers were compromised, and used to steal SSH credentials, and redirect web visitors to malicious content and send spam.

Provide an overview of this campaign, and the three main malicious components of this operation:

- **Linux/Ebury** – an OpenSSH backdoor used to keep control of the servers and steal credentials
- **Linux/Cdorked** – an HTTP backdoor used to redirect web traffic
- **Perl/Calfbot** – a Perl script used to send spam
The objective of this campaign is to gain monetary rewards.

It is done via the followings ways:

- Spam
- User’s infection via drive-by downloads
- Redirection of web traffic to advertisement networks
Timeline

2011 SEPTEMBER
kernel.org compromised with Linux/Ebury

2011 NOVEMBER
Steinar H. Gunderson publishes a first technical analysis of Linux/Ebury

2013 FEBRUARY
cPanel reports systems in their support department had been compromised with Linux/Ebury

2013 APRIL
A publication of the first technical analysis of Linux/Cdorked is made with Sucuri

2013 JUNE
The link between Linux/Ebury and Linux/Cdorked is made

2013 OCTOBER
Network traffic capture of Perl/Calfbot C&C reveals that an average of 35 million of spam messages are sent daily

2013 SEPTEMBER
Network traffic capture reveals more than 12,000 hosts infected with Linux/Ebury

2013 JULY
Network traffic capture on Linux/Cdorked redirection target reveals over 1 million malicious web redirections in two days

2014 JANUARY
A new related spam-sending malware is found: Perl/Calfbot
Timeline

- **September 2013**: ESET captures network traffic from a server infected by Linux/Ebury running a reverse proxy service used as a target for Linux/Cdorked redirections, revealing over 1,000,000 web redirections in 48 hours.

- **October 2013**: ESET captures 72 hours of network traffic revealing more than 12,000 servers infected with Linux/Ebury.

- **January 2014**: ESET captures network traffic during three distinct 24-hour periods from a server running both a Linux/Ebury exfiltration service and a Perl/Calfbot command and control reverse proxy, revealing an average of 35 million spam messages sent daily.
High Level Operation
Several piece of malware used in the campaign:

- **Linux/Ebury** runs mostly on Linux servers. It provides a root backdoor shell and has the ability to steal SSH credentials.

- **Linux/Cdorked** runs mostly on Linux web servers. It provides a backdoor shell and distributes Windows malware to end users via drive-by downloads.

- **Perl/Calfbot** runs on most Perl supported platforms. It is a lightweight spam bot written in Perl.

- **Win32/Boaxxe.G**, a click fraud malware, and **Win32/Glupteba.M**, a generic proxy, run on Windows computers. These are the two threats distributed via drive-by download.
# Relationship of Malware Components vs Activity/Service

<table>
<thead>
<tr>
<th>Malicious Activity</th>
<th>Malware Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam</td>
<td>Win32/Glupteba.M, Perl/Calfbot, Linux/Ebury</td>
</tr>
<tr>
<td>Drive-by downloads</td>
<td>Linux/Cdorked</td>
</tr>
<tr>
<td>Advertisement fraud</td>
<td>Linux/Cdorked, Win32/Boaxxe.G</td>
</tr>
<tr>
<td>Credential stealing</td>
<td>Linux/Ebury</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Malicious Infrastructure Service</th>
<th>Malware Component Involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam-related DNS services</td>
<td>Linux/Ebury with TinyDNS</td>
</tr>
<tr>
<td>Cdorked DNS services</td>
<td>Linux/Ebury with Linux/Onimiki</td>
</tr>
<tr>
<td>Credential exfiltration service</td>
<td>Linux/Ebury with additional binary component</td>
</tr>
<tr>
<td>Configuration service</td>
<td>Linux/Ebury</td>
</tr>
<tr>
<td>SSH tunnel</td>
<td>all infected with Linux/Ebury</td>
</tr>
<tr>
<td>Reverse proxy service</td>
<td>all infected with Linux/Ebury</td>
</tr>
<tr>
<td>Anonymizing tunnel</td>
<td>Linux/Ebury</td>
</tr>
</tbody>
</table>
High Level Operation

Sheer number of infected servers supporting the malicious activities

Two type of victims:
- Windows end-users visiting legitimate web sites hosted on compromised servers
- Linux/Unix servers operators whom servers were compromised

The malicious actors using these compromised servers to run one or more malicious services necessary for managing their whole operation
Credentials Stealing

Diagram showing the process of credentials stealing:

1. **Victim** uses a device.
2. SSH (Secure SHell) is used to connect to a server with Linux/Ebury.
3. **Clean server** is deployed using SSH.
4. DNS packet with credentials is sent to exfiltration servers.
5. **Exfiltration servers** collect credentials (every 5 minutes).
6. Anonymizing tunnel endpoint is used to collect passwords (twice a day).
7. Backdoor is connected to collect passwords.
8. Operator is involved in malicious activity.

Legend:
- Blue: Legitimate system/user
- Black: Involved in malicious activity
- Yellow: Infected with Linux/Ebury

**Note:** The diagram illustrates the steps involved in the credentials stealing process using SSH and DNS packets. The operator is involved in malicious activity, and the exfiltration servers collect credentials periodically. The clean server is deployed using SSH, and the device is used by the victim. The backdoor is connected to collect passwords, and the anonymizing tunnel endpoint is used to anonymize the traffic.
Credentials Stealing

Two scenarios SSH credentials are stolen:

- Successful logon of a user on a infected server
- User logon to another system using a compromised server

Linux/Ebury backdoor is use for stealing credential

Backbone of the Windigo operation
Credentials Stealing

- Credentials intercepted by Linux/Ebury send to exfiltration servers via custom DNS queries
- Used to further spread infection
- Criminal gang appear to have good operational security
- Never directly connect to any compromised server
- Used anonymizing tunnel on another compromised server
- Fetch stolen credentials stored on various infected servers
Infection Scenarios

User logs into a clean machine from a compromised server.

SSH
- Credentials leaked to Windigo operator

Root credentials?
- YES
  - Install Linux/EBury
  - Webserver hosted?
    - YES
      - Use as part of Windigo Infrastructure:
        - Linux/EBury exfiltration
        - Reverse proxy
        - Spam-related DNS services
        - SSH tunnel
        - Install Linux/conpinix
    - NO
      - Install Perl/orbot
      - Do nothing

- NO
  - Do nothing

Legitimate system/user
Involved in malicious activity
Infected with Linux/EBury
Infected with Linux/orbot
Infected with Perl/orbot
Linux/ Ebury Infected Hosts

<table>
<thead>
<tr>
<th>Capture Date</th>
<th>Count of Unique Infected IP addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 2013</td>
<td>7,707</td>
</tr>
<tr>
<td>October 2013</td>
<td>12,326</td>
</tr>
<tr>
<td>January 2014</td>
<td>11,110</td>
</tr>
</tbody>
</table>
# Top 5 Infected Countries

<table>
<thead>
<tr>
<th>Position</th>
<th>Country</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>United States</td>
<td>10,065</td>
</tr>
<tr>
<td>2</td>
<td>Germany</td>
<td>2,489</td>
</tr>
<tr>
<td>3</td>
<td>France</td>
<td>1,431</td>
</tr>
<tr>
<td>4</td>
<td>Italy</td>
<td>1,169</td>
</tr>
<tr>
<td>5</td>
<td>United Kingdom</td>
<td>993</td>
</tr>
<tr>
<td></td>
<td>Others</td>
<td>9,877</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>26,024</strong></td>
</tr>
</tbody>
</table>
Web Traffic Redirection

Infected web servers with Linux/Cdorked redirect users to exploit kit servers, which in turn attempt to infect users with malware.

This malicious action follows the below steps:

1. Victim visits a legitimate website, which is a Linux/Cdorked infected server. Victim is being redirected to a specially crafted subdomain of a legitimate domain name.

2. The nameserver of the legitimate domain, infected with another component of the Windigo operation named Linux/Onimiki, returns an IP address encoded in the subdomain. Thus, it allows the Windigo operation to make use of legitimate nameservers, making network-based detection harder.

3. Reverse proxy servers on exploit serving machines are used to exploit victims, if successful, deliver malicious payload to victims; failing which, victims are redirected to advertisements.
Stolen SSH Passwords

- Monitored data sent to exfiltration servers

- 5,362 unique successful logins from 2,840 different IP addresses

- No surprise a large number of root credentials are stolen, as malware must be installed as root.

- The higher number of root passwords, result in higher number of infections

- Vicious cycle resulting in greater chances of stealing other root credentials
# Statistics SSH Passwords

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of unique passwords</td>
<td>2,145</td>
</tr>
<tr>
<td>Number of passwords containing only alphabetic characters</td>
<td>190</td>
</tr>
<tr>
<td>Number of passwords containing only numeric characters</td>
<td>36</td>
</tr>
<tr>
<td>Number of passwords containing only alphanumeric characters</td>
<td>1,422</td>
</tr>
<tr>
<td>Number of passwords with special characters (non alphanumeric)</td>
<td>723</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>3</td>
</tr>
<tr>
<td>Maximum password length</td>
<td>50</td>
</tr>
<tr>
<td>Median password length</td>
<td>10</td>
</tr>
<tr>
<td>Average number of characters in a password</td>
<td>11.1</td>
</tr>
</tbody>
</table>
Statistics SSH Passwords

- Average length of password is 11.09 characters, much longer than the 7.63 average discovered in LulzSec leak in 2011.
- Shows that system administrators are more conscious on importance of strong password.
- Passwords are well chosen, and generally do not contain repeating patterns.
- 33% of passwords contain at least one special character and average length of 11 characters.
- This is generally secure against brute force attempts.
One way the Windigo operators are monetizing through this campaign is by sending spam email.

Two methods are used:
- Servers infected with Perl/Calfbot
- End-user workstations infected with Win32/Glupteba.M

We used two approaches to understand the volume and type of spam send via the Perl/Calfbot infrastructure, namely:

- Fake Bot
- C&C Traffic Analysis
Fake Bot

- Analysis period from August 2013 to February 2014
- A fake client is used to fetch spam jobs from C&C server
- Spam jobs consists of multiple email templates and list of recipient email addresses
- Fake Bot retrieved 13,422 different spam jobs targeting 20,683,814 unique email addresses
Fake Bot

<table>
<thead>
<tr>
<th>Position</th>
<th>Country</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>France</td>
<td>2,050,872</td>
</tr>
<tr>
<td>2</td>
<td>United Kingdom</td>
<td>1,483,725</td>
</tr>
<tr>
<td>3</td>
<td>Russia</td>
<td>854,580</td>
</tr>
<tr>
<td>4</td>
<td>Germany</td>
<td>458,041</td>
</tr>
<tr>
<td>5</td>
<td>Italy</td>
<td>333,204</td>
</tr>
<tr>
<td></td>
<td>Others</td>
<td>2,271,782</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>7,452,204</strong></td>
</tr>
</tbody>
</table>
C&C Traffic Analysis

- Analysed network traffic captured on 1 C&C servers over 24-hour period over 3 weeks for the month of January 2014
- Infected servers reported daily average of 35 million successful spam messages

<table>
<thead>
<tr>
<th>Date</th>
<th>IP addresses</th>
<th>Active IP addresses (% of total)</th>
<th>Spam sent (average per active IP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 7</td>
<td>1,442</td>
<td>244 (17 %)</td>
<td>27,713,339 (113,579)</td>
</tr>
<tr>
<td>Jan 14</td>
<td>483</td>
<td>300 (62 %)</td>
<td>32,793,722 (109,312)</td>
</tr>
<tr>
<td>Jan 24</td>
<td>877</td>
<td>490 (56 %)</td>
<td>46,402,673 (94,699)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Position</th>
<th>Country</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>United States</td>
<td>309</td>
</tr>
<tr>
<td>2</td>
<td>Germany</td>
<td>72</td>
</tr>
<tr>
<td>3</td>
<td>Russia</td>
<td>41</td>
</tr>
<tr>
<td>4</td>
<td>United Kingdom</td>
<td>32</td>
</tr>
<tr>
<td>5</td>
<td>Turkey</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Others</td>
<td>258</td>
</tr>
<tr>
<td></td>
<td><strong>Total</strong></td>
<td>735</td>
</tr>
</tbody>
</table>
Redirected End Users

- Through analysis of network traffic captured from a reverse proxy, we observed more than 1.1 million different IP addresses going through this server, and being redirected to exploit kit servers.

- When a user's computer is redirected to a front-end reverse proxy, it starts a series of back-and-forth communications with the exploit kit server. In the end, user's computer may be infected with malware if it is vulnerable to the exploit.

- The Blackhole kit was used by Windigo operators here, targeting Windows users. In October 2013, the operators switched to Neutrino exploit kit, after the arrest of alleged Blackhole author. In March 2014, we observed the use of Flashback.

- Two distinct malware families were distributed by the exploit kit. Specifically from USA, UK, Canada and Australia were infected with Win32/Boaxxe.G, whereas others were infected with Win32/Leechole, a dropper which then installed Win32/Glupteba.M.
Redirected End Users

- **Blackberry**: 8,081
- **Linux**: 7,726
- **Windows Vista**: 24,997
- **Windows Phone**: 4,821
- **OS X**: 35,135
- **Unknown**: 49,676
- **Windows 8**: 51,020
- **Windows 7**: 364,224
- **iOS**: 182,329
- **Android**: 225,596
- **Windows Server**: 202,711
- **Chrome OS**: 334
- **Windows 8.1**: 238
- **Other**: 1,794

**ESET**

ENJOY SAFER TECHNOLOGY™

28
The purpose of the operation seems to be monetary profit. This profit is gathered through various ways including redirecting web users to malicious content and sending unsolicited emails.

From this presentation, we hope to reach out to the general public, the researcher community and system administrators who had the responsibility of managing of servers on the Internet.

One message we would like reader/audiences to take away is that:

Password-based login to servers should be a thing of the past. One should seriously consider two-factor authentication or, at least, a safe use of SSH keys.
ESET Blog: www.welivesecurity.com

Operation Windigo:
http://www.welivesecurity.com/2014/03/18/operation-windigo-the-vivisection-of-a-large-linux-server-side-credential-stealing-malware-campaign/


Indicators of Compromise:
https://github.com/eset/malware-ioc

For any technical inquiries please contact:
windigo@eset.sk