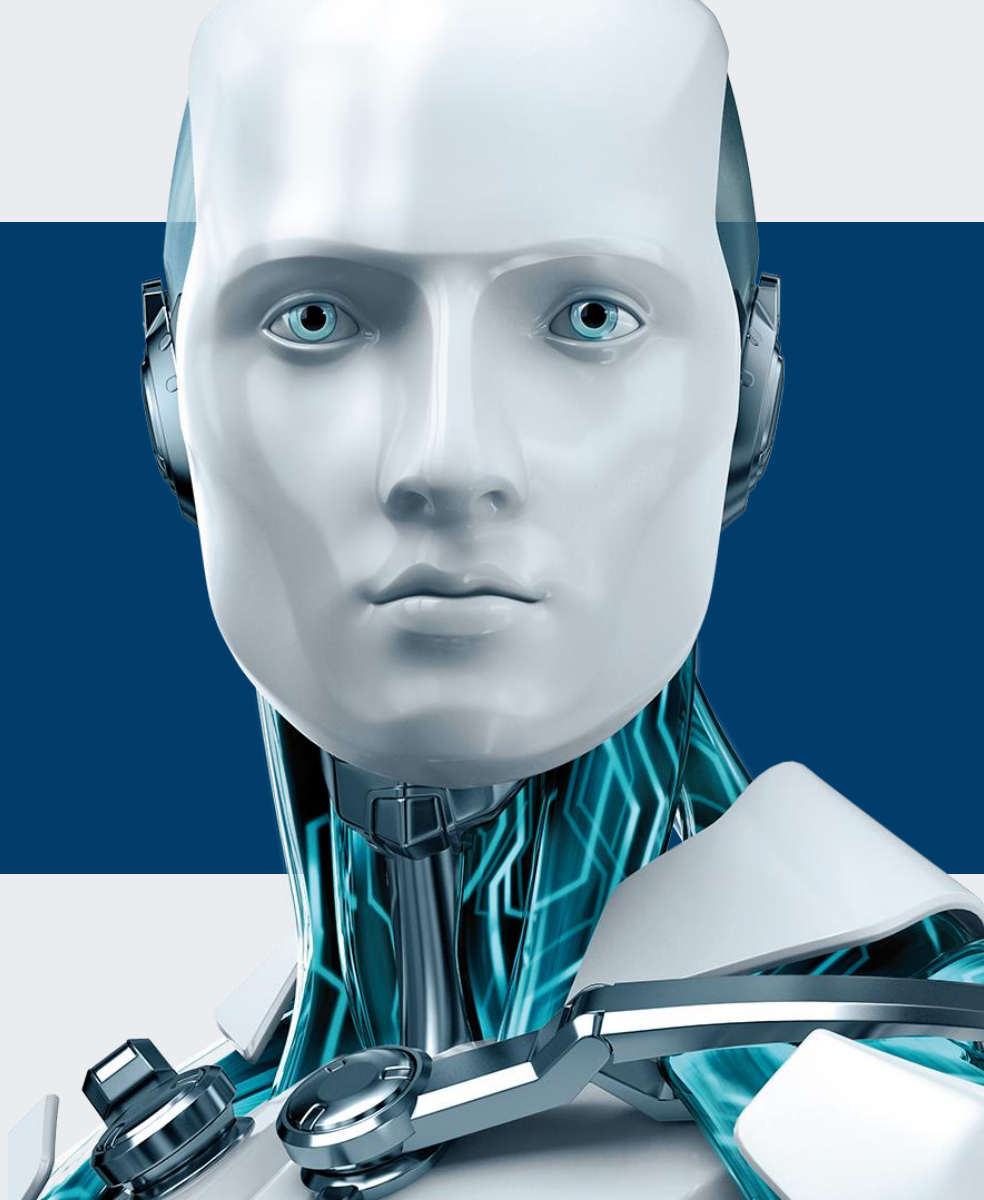
OPERATION WINDIGO

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



Oh Sieng Chye, Researcher
ESET ASIA (Singapore)

ESET ENJOY SAFER TECHNOLOGY™

ESET Researchers Acknowledgement

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

Introduction

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

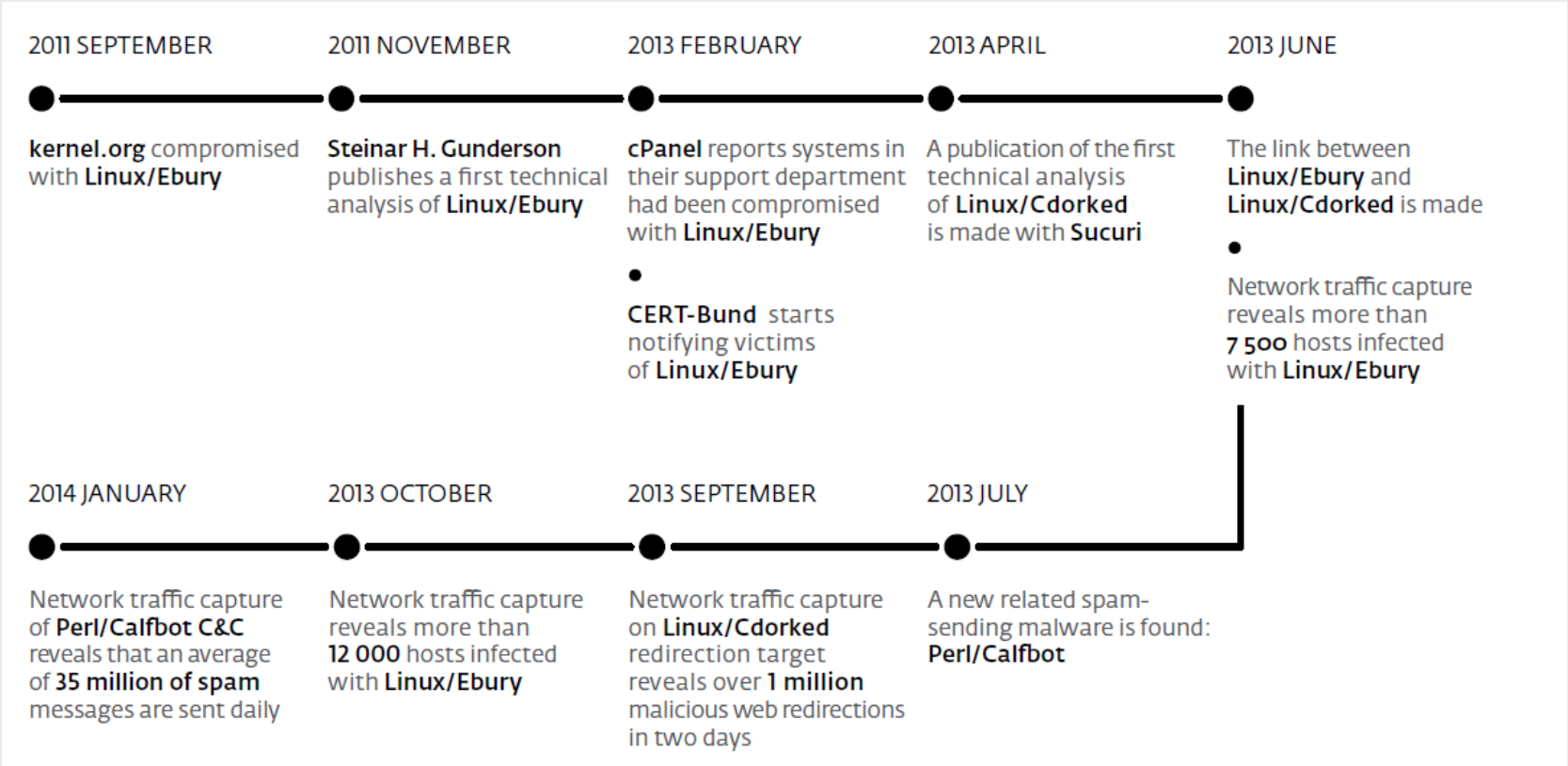
Introduction

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
CERT-Bund starts notifying victims of 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
Network traffic capture reveals more than 7 500 hosts infected with Linux/Ebury
2013 JULY
A new related spam-sending malware is found: Perl/Calfbot
2013 SEPTEMBER
Network traffic capture on Linux/Cdorked redirection target reveals over 1 million malicious web redirections in two days
2013 OCTOBER
Network traffic capture reveals more than 12 000 hosts infected with Linux/Ebury
2014 JANUARY
Network traffic capture of Perl/Calfbot C&C reveals that an average of 35 million of spam messages are sent daily

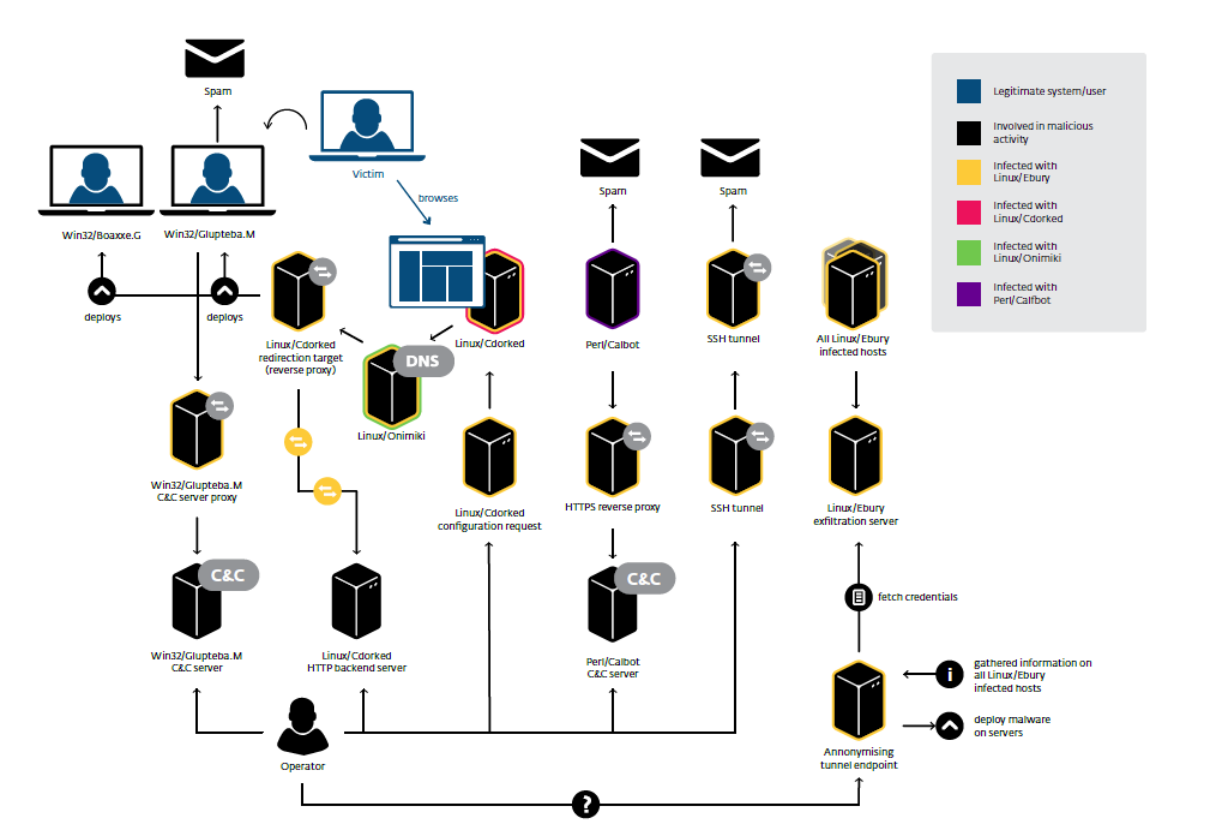
Timeline

- 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



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

Malicious Activity	Malware Component
Spam	Win32/Glupteba.M, Perl/Calfbot, Linux/Ebury
Drive-by downloads	Linux/Cdorked
Advertisement fraud	Linux/Cdorked, Win32/Boaxxe.G
Credential stealing	Linux/Ebury

Malicious Infrastructure Service	Malware Component Involved
Spam-related DNS services	Linux/Ebury with TinyDNS
Cdorked DNS services	Linux/Ebury with Linux/Onimiki
Credential exfiltration service	Linux/Ebury with additional binary component
Configuration service	Linux/Ebury
SSH tunnel	all infected with Linux/Ebury
Reverse proxy service	all infected with Linux/Ebury
Anonymizing tunnel	Linux/Ebury

High Level Operation

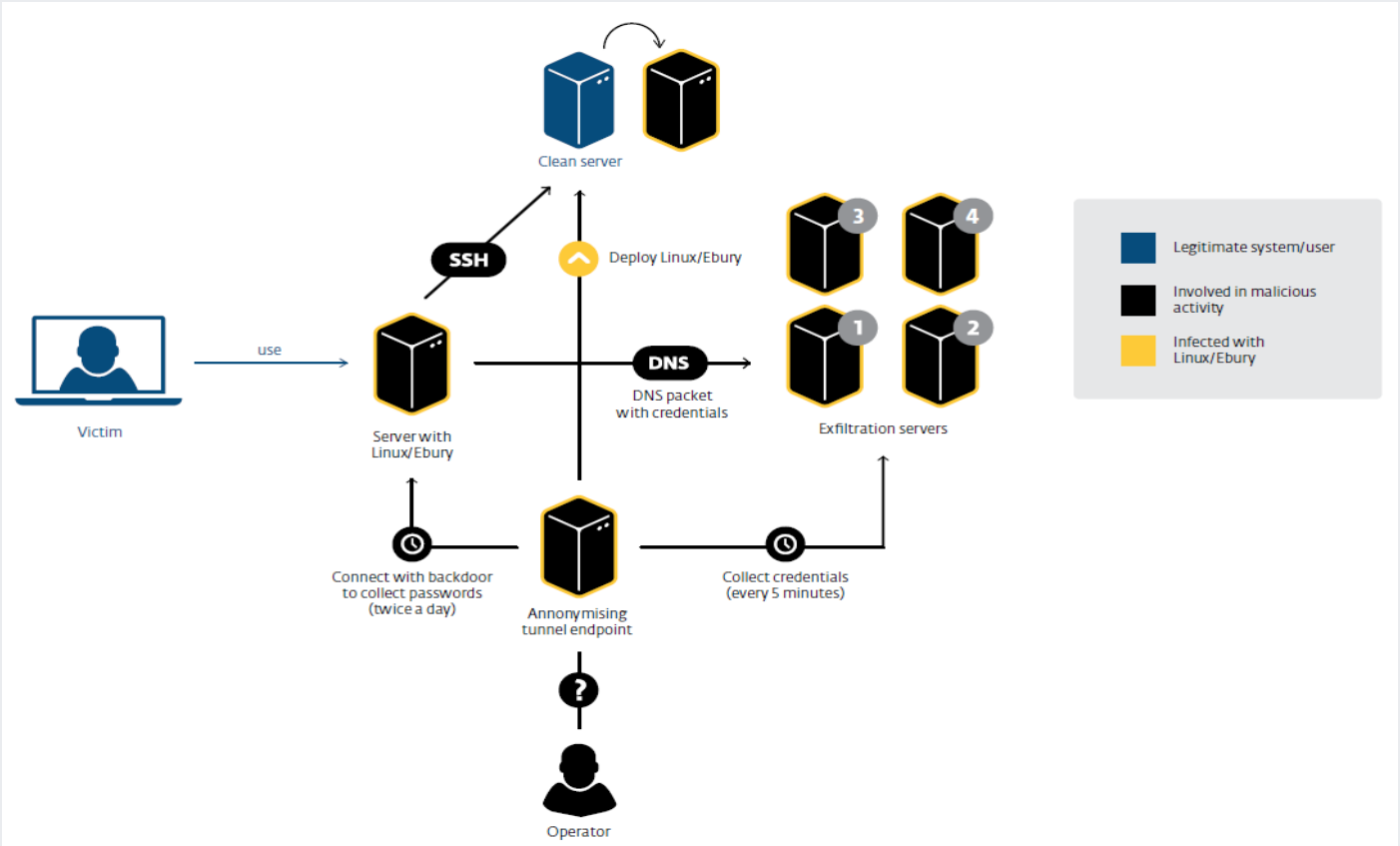
Sheer number of infected servers supporting the malicious activities

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



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

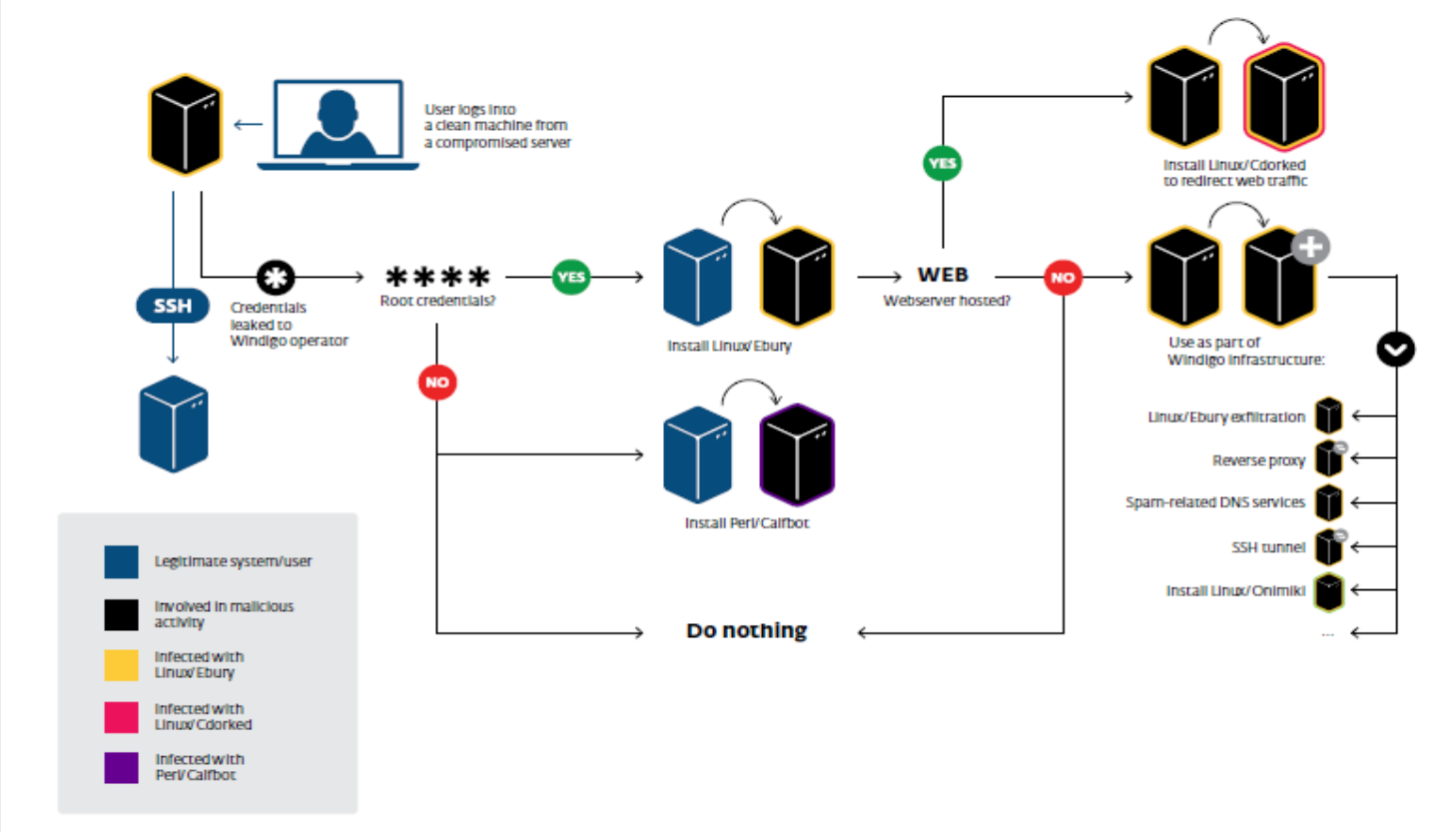
Linux/Ebury backdoor is use for stealing credential

Backbone of the Windigo operation

Credentials Stealing

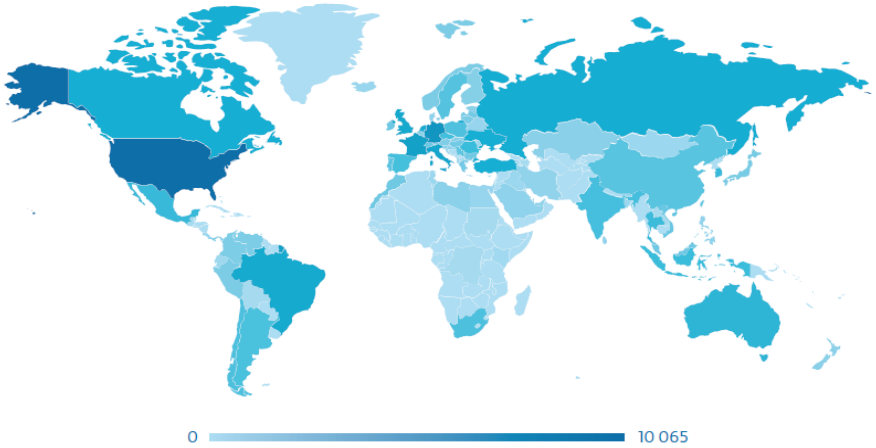
- Credentials intercepted by Linux/Ebury send to exfiltration servers via custom DNS queries
- Used to further spread infection
- Criminal gang appear to have good operational security
- Never directly connect to any compromised server
- Used anonymizing tunnel on another compromised server
- Fetch stolen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

Infection Scenarios



Linux/ Ebury Infected Hosts

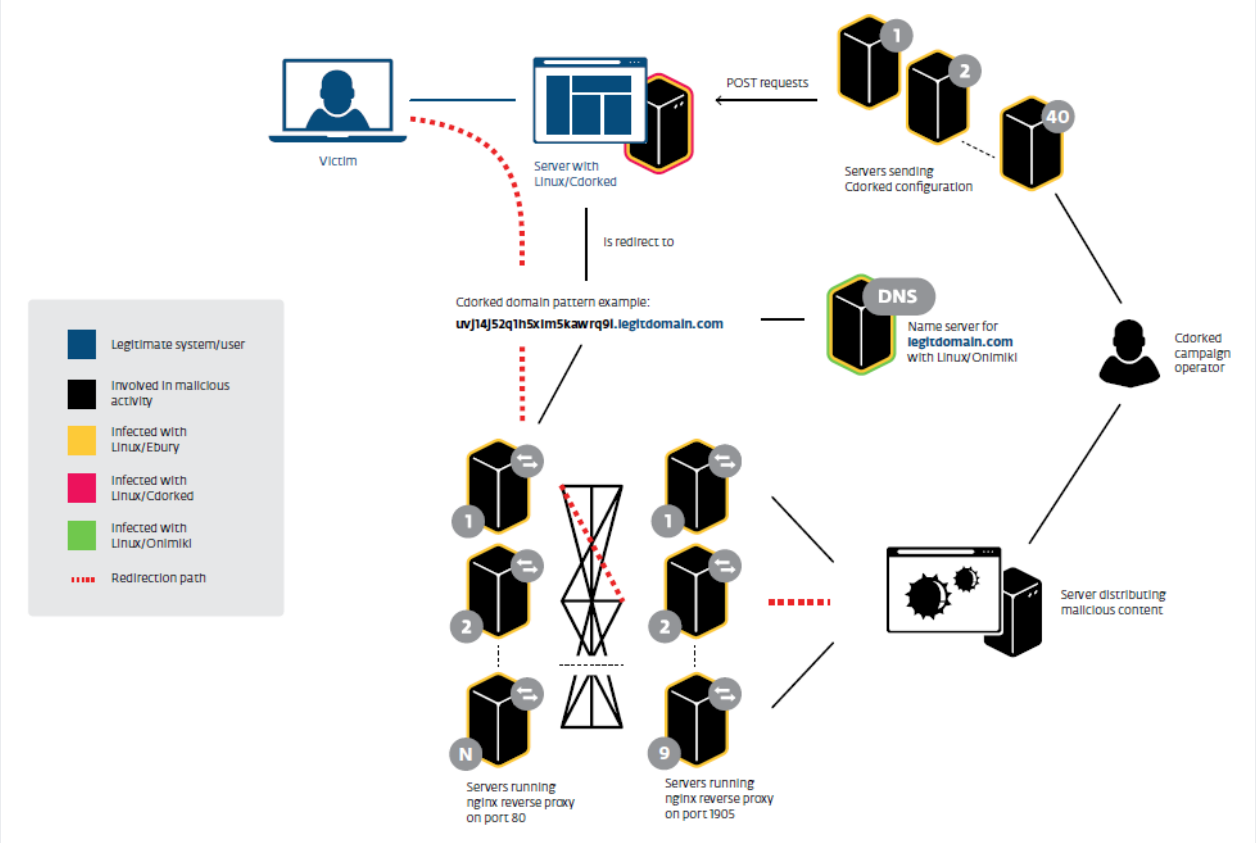
Capture Date	Count of Unique Infected IP addresses
June 2013	7,707
October 2013	12,326
January 2014	11,110



Top 5 Infected Countries

Position	Country	Count
1	United States	10,065
2	Germany	2,489
3	France	1,431
4	Italy	1,169
5	United Kingdom	993
	Others	9,877
Total		26,024

Web Traffic Redirection



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 address
- 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

Number of unique passwords	**2,145**
Number of passwords containing only alphabetic characters	190
Number of passwords containing only numeric characters	36
Number of passwords containing only alpha numeric characters	1,422
Number of passwords with special characters (non alpha numeric)	723
Minimum password length	3
Maximum password length	50
Median password length	10
Average number of characters in a password	11.1

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

Spam Analysis

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

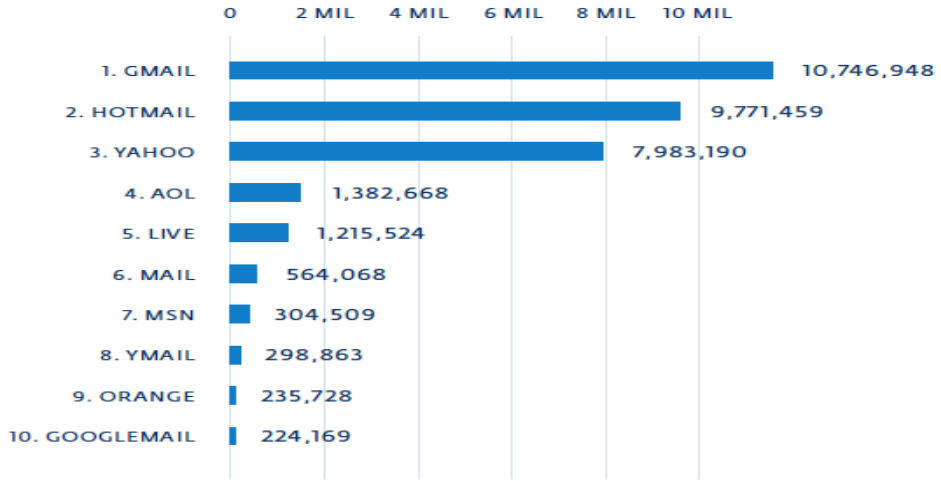
We used two approaches to understand the volume and type of spam send via the Perl/Calfbot infrastructure, namely:

- 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



Position	Country	Count
1	France	2,050,872
2	United Kingdom	1,483,725
3	Russia	854,580
4	Germany	458,041
5	Italy	333,204
	Others	2,271,782
Total		7,452,204

C&C Traffic Analysis

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

Position	Country	Count
1	United States	309
2	Germany	72
3	Russia	41
4	United Kingdom	32
5	Turkey	23
	Others	258
Total		735

- 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

Redirected End Users

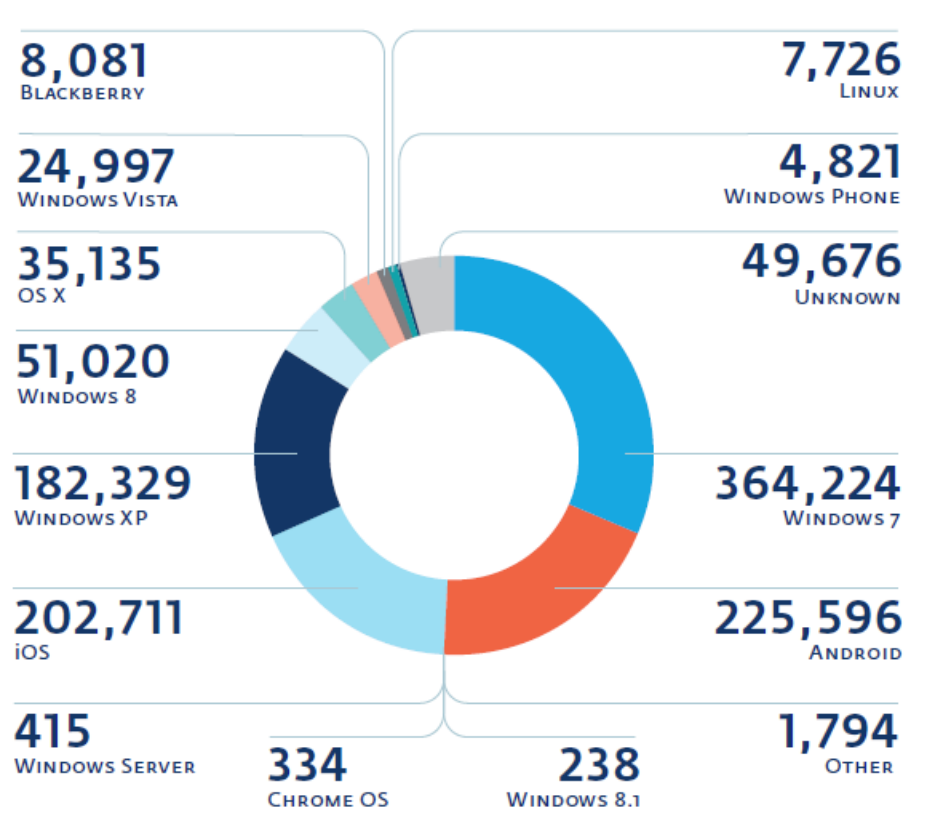
- Through analysis of network traffic captured from a reverse proxy, we observed more than 1.1 million different IP addresses going through this server, and being redirected to exploit kit servers.

- 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

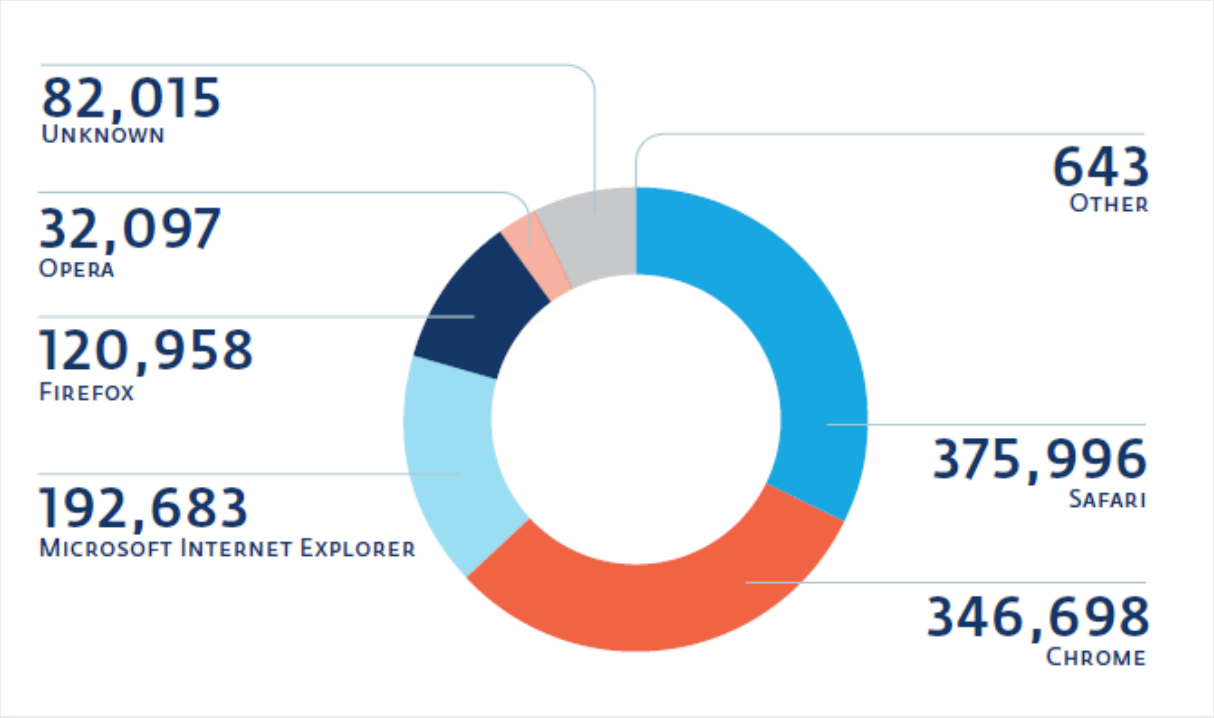
- The Blackhole kit was used by Windigo operators here, targeting Windows users. In October 2013, the operators switched to Neutrino exploit kit, after the arrest of alleged Blackhole author. In March 2014, we observed the use of Flashback

- 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



Redirected End Users



NOT the end……

- 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.

More details……

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/

White Paper: http://www.welivesecurity.com/wp-content/uploads/2014/03/operation_windigo.pdf

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

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