Operation Windigo: “Good job, ESET!” says malware author

welivesecurity.com/2014/10/15/operation-windigo-good-job-eset-says-malware-author/

October 15, 2014

Following the recognition at Virus Bulletin 2014 of ESET’s research on Operation Windigo, I took the opportunity to ask Marc-Etienne Léveillé – who worked directly on the Operation Windigo report a few questions. Marc-Etienne is a malware researcher at ESET.

Olivier Bilodeau
15 Oct 2014 - 12:00PM

Following the recognition at Virus Bulletin 2014 of ESET’s research on Operation Windigo, I took the opportunity to ask Marc-Etienne Léveillé – who worked directly on the Operation Windigo report a few questions. Marc-Etienne is a malware researcher at ESET.

Following the recognition at Virus Bulletin 2014 of ESET’s research on Operation Windigo, I took the opportunity to ask Marc-Etienne Léveillé – who worked directly on the Operation Windigo report a few questions. Marc-Etienne is a malware researcher at ESET. He is interested in reverse engineering Linux and OS X malware. He is passionate about making links between different malware to have an overall view of how they are interconnected.

Quite some time has passed since you last spoke about the large Linux crimeware operation dubbed Operation Windigo. Has there been anything happening lately worth of mention?

We are still monitoring the Windigo gang. Unfortunately, we have not observed a decrease in their malicious activities since the publication of the report in March 2014. We still measure and block the same amount of traffic being redirected from Cdorked websites. Moreover, the various pieces of malware have been updated to evade our indicators of compromise (IoC).

What is the biggest challenge posed by threats like these to system administrators?

We have been notifying a lot of infected parties and I would say that the lack of Linux forensic knowledge is the main problem for sysadmins. Windigo uses a lot of tricks to stay under the radar. Since it doesn’t interrupt the affected server’s legitimate activity, such a server could be infected for a very long time before the administrator notices the infection. Some sysadmins may stay in denial and refused to believe their server is infected.

What does the ESET research team do to raise the awareness of the issue?

We are trying to reach out to the security community to help sites with Internet-facing servers protect themselves against the Windigo threat, and against other general purpose Linux malware overall. An effective way to do so is to get the opportunity to speak directly to system administrators and security researchers who are front-line defenders against such threats. That’s why we were so happy to present on the topic at DerbyCon and, in collaboration with Yandex, at Virus Bulletin.

In the near future we will be presenting at the following conferences:

- LinuxCon Europe, October 15th, Düsseldorf, Germany
- SecTor, October 22nd, Toronto, Canada
- CSAW:Threads, November 13-14th, New York, USA
- conf.au, January 16th, Auckland, New Zealand

If your readers would like to know more about Operation Windigo or Linux malware reverse-engineering, forensics and incident response please come and talk to us.

What kind of changes were introduced in the recent versions of the Linux/Ebury malware?

The authors of the Ebury malware react quite quickly to our publications. Within a month, we've seen a new version of the malware evading our indicators of compromise. Here are a few of the most noticeable changes:

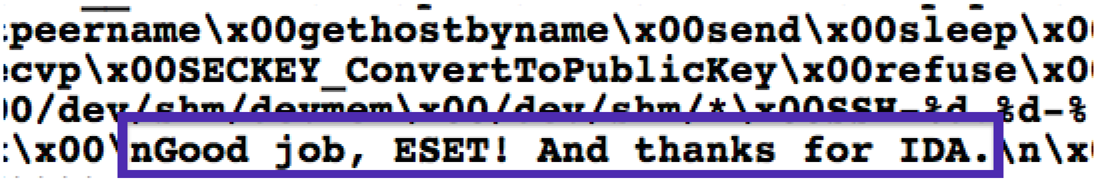
- The version number has jumped to 1.5.1 (which is the latest version number that we've seen). We also saw version 1.4.1 for the first time in April 2014. At the time we released the Operation Windigo report in March, the latest version observed had been 1.3.5.
- Ebury no longer uses shared memory for storing stolen credentials and maintaining inter-process communication. Instead, a new process is started and injected with the Ebury payload with LD_PRELOAD. Stolen credentials are kept in this new process address space. Inter Process Communication (IPC) with OpenSSH is initiated over a UNIX domain socket.
- The domain name generator algorithm (DGA) used as a backup to exfiltrate credentials has changed. This backup is used when it has not been configured by the operator.
- Version 1.5 no longer infects the so file directly. The Ebury payload is located in a new file in the library directory with the filename libns2.so. The system's original libkeyutils.so is then patched to link to this new malicious library instead of libc.so.6. The Ebury code will then be loaded and hook OpenSSH.

Using this new information gleaned from our monitoring, CERT-Bund has updated its page with the Ebury IOCs.

In addition to the "Good job, ESET!" from the malware authors, your team has won the first Virus Bulletin Péter Szőr award for your report on Operation Windigo. How does that make you feel?

There were a lot of excellent papers on malware research this year and I would like to give credit and respect to the other nominees and to *all* the researchers who have published great work in the last years.

In addition to what was said before, I would like to acknowledge that most of the co-authors and researchers involved in the Operation Windigo paper are newcomers to the anti-virus industry. For us, receiving an award like this is much appreciated recognition from our peers and gives us confidence that we are heading in the right direction.



```
:peername\x00gethostbyname\x00send\x00sleep\x0
:cvp\x00SECKEY_ConvertToPublicKey\x00refuse\x0
)0/dev/shm/devmem\x00/dev/shm/*\x00SSH-%d.%d-%
:\x00\nGood job, ESET! And thanks for IDA.\n\x
```

Recognition of ESET’s work by malware authors

Our first priority is to protect our customers against all threats, including new and emerging ones. As a researcher, it is great to be able to focus deeply on a specific threat like this one. Thanks to ESET’s belief in proper research, we were able to really do a deep investigation and protect our customers at the same time. We are really pleased it was so well received by the press, our customers and Virus Bulletin.

Thanks Marc-Etienne for your time.

15 Oct 2014 - 12:00PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion