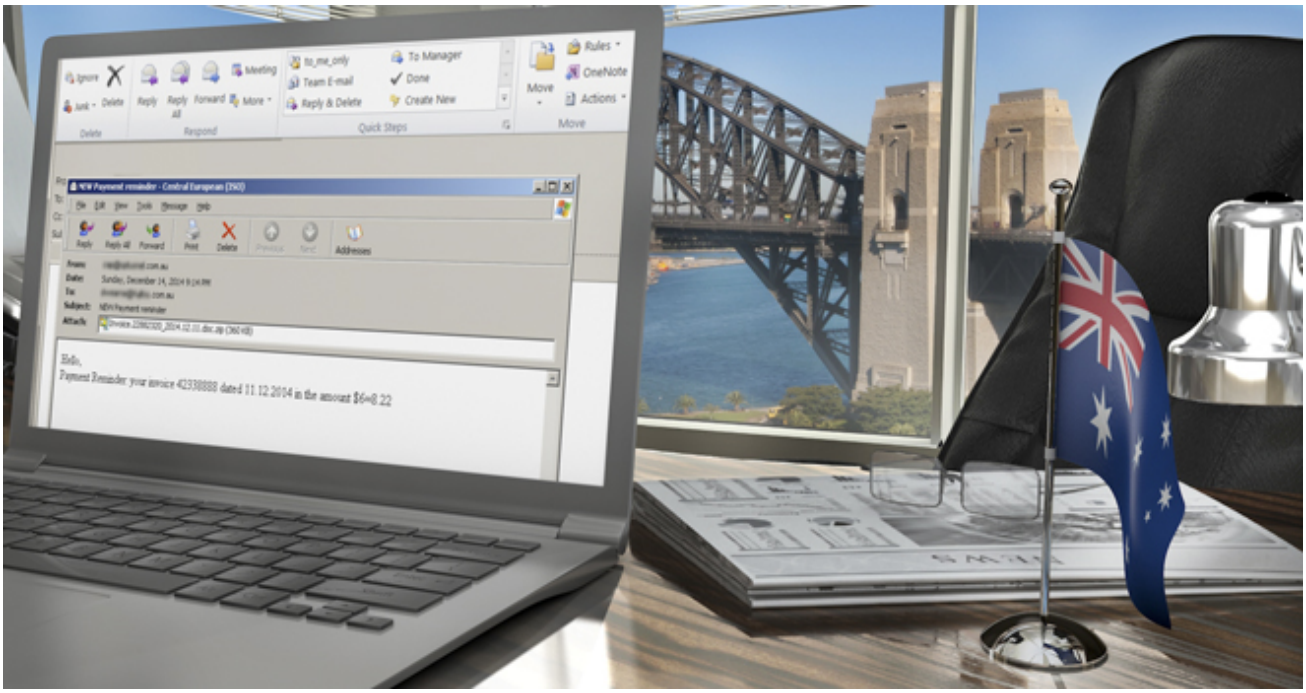
Endpoint Protection

symantec.com/connect/blogs/new-carberp-variant-heads-down-under

Jan 13, 2015 05:00 PM

Migration User



When the source code for the botnet creation kit known as Carberp (Trojan.Carberp) was leaked in June 2013, security experts predicted it would only be a matter of time before the information-stealing malware code would be modified and reused. Those experts were proven right when Trojan.Carberp.B was uncovered in late 2014. Symantec has now observed yet another modified version of Carberp (Trojan.Carberp.C) being spread through a spam campaign mainly targeting Australia.

This latest version of the malware is still focused on stealing information and has the ability to download additional plugins that add to its functionality.

The Carberp malware likes to travel, it would seem. In its early days, Carberp was exclusively used to swipe online banking credentials and other valuable information in Russian-speaking countries but was later modified to allow the malware to target US banks.

Just like any successful business, expansion is the key and now Carberp is exploring yet another continent.

The fact that the new variant is mainly targeting Australia may also point to a wider trend in malware authors venturing into the land down under, as recently highlighted by a significant increase in cryptomalware hitting Australian computers.

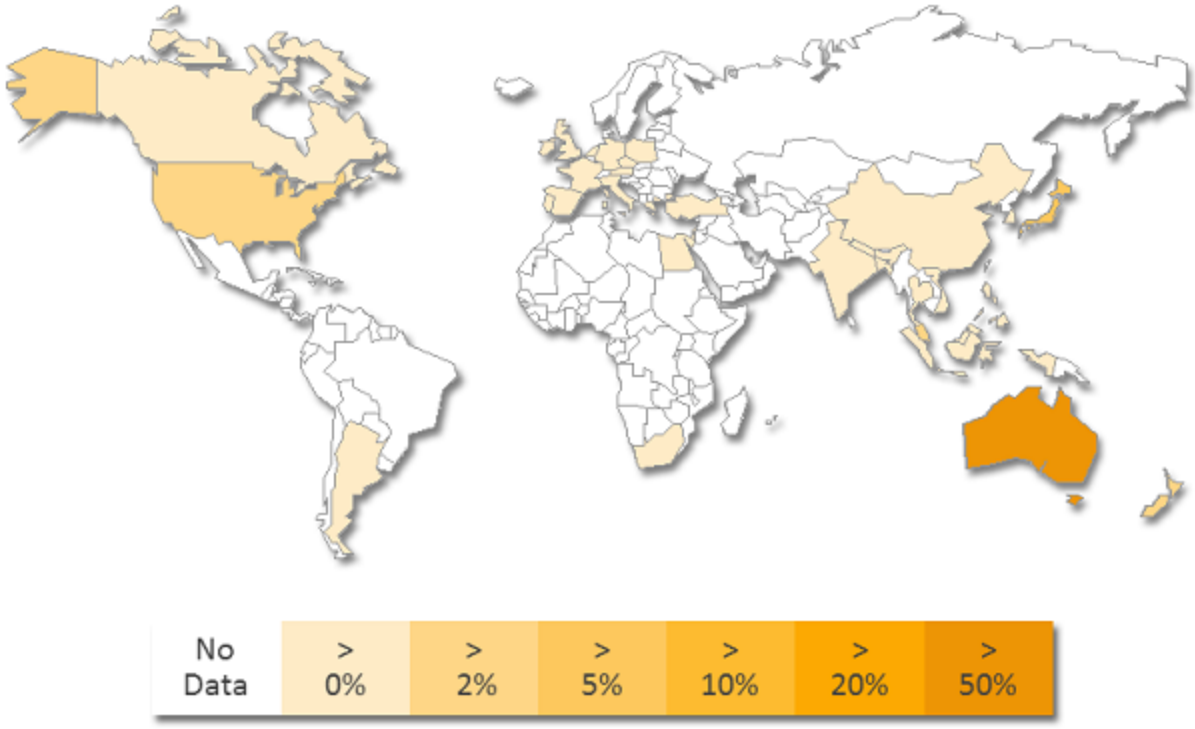


Figure 1. Carberp variant mainly targeting Australia

Analysis

The spam email used to spread Trojan.Carberp.C claims to be a payment reminder and includes an attachment that poses as an invoice. The following is an example of the file name normally used for the attachment:

invoice.[RANDOM NUMBERS]_2014.12.11.doc.zip

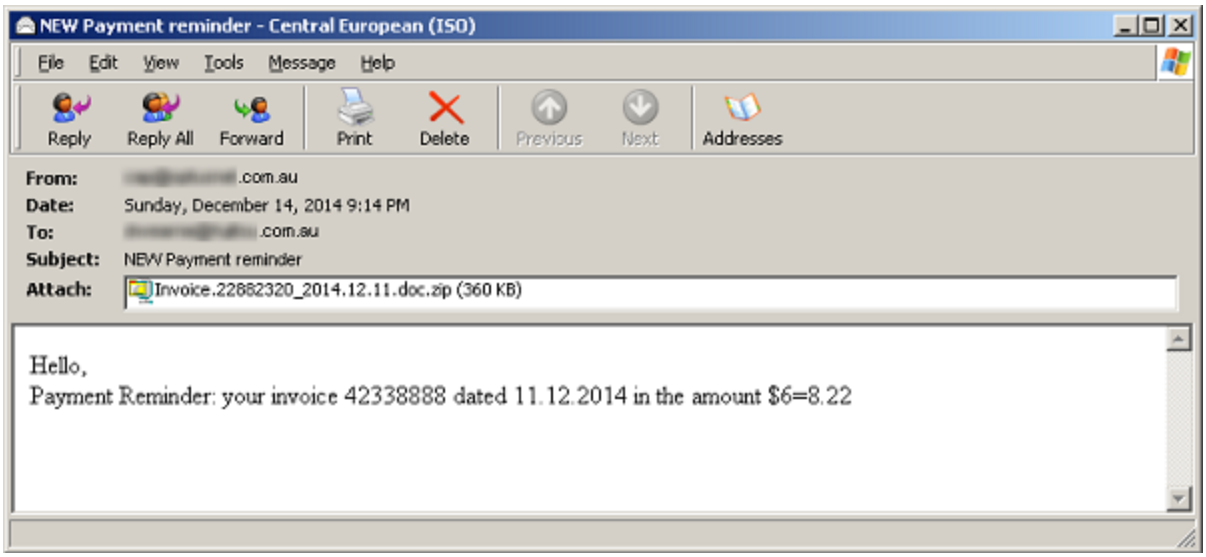


Figure 2. Spam email with malicious attachment

As you've probably already guessed, the attachment isn't an invoice and is actually malware packed with Visual Basic. Interestingly, after discovering this spam campaign on December 15, 2014, we noticed during our analysis that the compilation date of the malware was just one day previous on December 14. The malware authors obviously didn't waste much time between coding up and releasing (however, this date can't always be trusted).

```
File Header
  Machine:                      014C (I386)
  Number of Sections:           0003
  TimeDateStamp:                548D6495 -> Sun Dec 14 10:21:09 2014
  PointerToSymbolTable:         00000000
  NumberOfSymbols:              00000000
  SizeOfOptionalHeader:         00E0
  Characteristics:              010F
```

Figure 3. Malware compilation date

What's interesting about this Carberp variant is the number of components involved in the attack, which are used to hide the infection and to silently download additional encrypted payloads that are then injected stealthily into processes. Additional components are embedded in the dropper (detected as Trojan.Dropper) and compressed.

The attackers behind this threat know that 64-bit architecture is now becoming the standard so they embedded components that are able to infect both 32-bit and 64-bit computers, a tactic that is increasingly common, as seen in other threats such as W64.Xpiro and Trojan.Poweliks.

In Carberp.C, we identified the following embedded components:

- MyFault—A Windows driver developed by Sysinternals that is normally used to trigger system crashes. This module on its own is not malicious and is used for troubleshooting. But the malware authors may have implemented it in order to trigger a blue screen of death (BSoD) in case the malware is being analyzed.

- Downloader—A silent payload downloader (detected as Trojan.Carberp.C)
- Carberp Driver—Can be used to kill processes and to inject into memory malicious payloads with the aim to hide the infection (detected as Trojan.Carberp.C)

A typical attack scenario works in the following way:

1. User receives a spam email and opens the malicious attachment which executes the Trojan
2. The Trojan injects code into a Windows process and decrypts and decompresses embedded 32-bit or 64-bit modules (depending on the operating system)
3. The Trojan then contacts the command-and-control (C&C) server with information about the infection and requests additional 32-bit or 64-bit payloads (depending on the operating system)
4. The payload is then downloaded, decrypted, and loaded into memory so that it is not visible

As I've already noted, the malicious attachment drops additional components (32-bit or 64-bit) depending on the computer architecture. These malicious files will contact the C&C server and send back details from the compromised computer such as:

- File system type
- User name of user that executed the malware
- Name and path of the executed file
- Time and date of the infection
- Process ID and parent PID

The malware is also able to download additional plugins that are injected into a newly created svchost.exe process in order to keep the infection hidden. We were able to identify plugins for different CPU architecture such as the following:

- host.dat
- update.dat
- [VOLUME SERIAL NUMBER]_32.dat
- [VOLUME SERIAL NUMBER]_64.dat
- list32.dat
- list64.dat

During our analysis, we were able to download list32.dat, which is a plugin used to hook specific APIs in order to steal confidential information such as user names and passwords from different internet browsers.

Symantec and Norton protection
Symantec advises users to be cautious when dealing with suspicious emails and to avoid clicking on suspicious links or opening attachments in unsolicited email.

Symantec has the following detections in place to protect against this threat:

Antivirus:

- Trojan.Dropper
- Trojan.Carberp.C

Intrusion prevention system: