Endpoint Protection

symantec.com/connect/blogs/flamer-recipe-bluetoothache

May 31, 2012 07:29 PM

A L Johnson

W32.Flamer is possibly the only Windows based threat we have encountered which uses Bluetooth. It is yet another indicator that W32.Flamer is not only exceptional, but that it is a comprehensive information gathering and espionage tool. The CrySyS laboratory has previously documented the technical details of Bluetooth in W32.Flamer. But, what does this actually mean for potential victims targeted by Flamer? What can an attacker accomplish using Bluetooth?

The Bluetooth functionality in Flamer is encoded in a module called "BeetleJuice". This module is triggered according to configuration values set by the attacker. When triggered it performs two primary actions:

1. The first is to scan for all Bluetooth devices in range. When a device is found, its status is queried and the details of the device recorded—including its ID—presumably to be uploaded to the attacker at some point.

2. The second action is to configure itself as a Bluetooth beacon. This means that a computer compromised by W32.Flamer will appear when any other Bluetooth device scans the local area. And there is more. In addition to enabling a Bluetooth beacon, Flamer encodes details about the infected computer (see Figure 1) and then stores these details in a special 'description' field. When any other device scans for Bluetooth-enabled devices, this description field will be displayed:

These are the facts of how Flamer uses Bluetooth. And what can the attacker do with this functionality? There are several potential avenues available:

Scenario #1 – Identification of victim social networks

By continuously monitoring the Bluetooth devices within range of a W32.Flamer compromised computer, the attacker can build a profile of various devices encountered throughout the day. This will be particularly effective if the compromised computer is a laptop because the victim is more likely to carry it around. Over time, as the victim meets associates and friends, the attackers will catalog the various devices encountered, most likely mobile phones. This way the attackers can build a map of interactions with various people—and identify the victim's social and professional circles.

Scenario #2 – Identification of victim physical locations

When compromising a victim's computer, the attacker has determined that this particular victim and their location is a high-priority target. While the building that the victim resides in can be known, the actual office is not identified. The attacker, however, could identify the location of compromised devices using Bluetooth.

Bluetooth operates over radio waves. By measuring the strength of a radio wave signal, an attacker can measure if he is she is getting closer or further away to a particular device. With the Bluetooth beacon turned on, and with the details of a particular compromised device available in the description field, it is straightforward for the attacker to identify the physical location of a W32.Flamer compromised computer or device.

An alternative to this is that rather than identifying the actual compromised computer, the attacker identifies a mobile phone which belongs to the victim. The Beetlejuice module already has retrieved a list of all the devices IDs which are near to the infected computer and so the attacker knows what devices belong to the victim. It is likely that one of the devices is a mobile phone which the victim carries most times. Now the attacker has the ability to passively monitor for the victim, without installing or modifying the victim's devices. Bluetooth monitoring devices could be placed in airports, train stations, or any transport hub, and listen for the ID values of any known victim device. Some attacks have even identified Bluetooth devices more than one mile away. The more sinister aspect of this passive sniffing is that it allows the attacker to pinpoint a victim and, therefore, more easily track them in the future.

Scenario #3 – Enhanced information gathering

As described in our previous blog, a substantial part of Flamer’s functionality is implemented in Lua scripts, or 'apps' which are downloaded from the FLAME 'app repository’. It would be trivial for an attacker to upload a new malicious Bluetooth Lua app

into the FLAME store for download onto a compromised device. With increase functionality an attacker, having identified various Bluetooth devices in range, could perform numerous attacks:

- Steal contacts from an address book, steals SMS messages, steals images, and more.
- Use a device to eavesdrop. Connect a compromised computer to a nearby device and enable handsfree communication. When the device is brought into a meeting room, or used to make a call, the attackers could listen in.
- Exfiltrate already-stolen data through any nearby device's data connection. This would bypass any firewalls or network controls. An attacker within one mile of the target could use their own Bluetooth-enabled device for this.

It is possible that there is undiscovered code within W32.Flamer which already achieves some of these goals. For example, although we have not found network code near the 'beacon' code, one compromised computer may connect to another computer using Bluetooth. If the second computer is using a secured network and was infected through a USB connection, potentially the only network available would be a Bluetooth connection back to the first compromised computer. The code to achieve this may already exist in Flame.

The various theories described here are all practical attacks, easily to implement by a skilled attacker. The sophistication of W32.Flamer indicates that the attackers are certainly technically skilled and such attacks are well within their capabilities.