Endpoint Protection

symantec.com/connect/blogs/w32narilam-business-database-sabotage

Nov 22, 2012 05:39 AM

A L Johnson

In the last couple of years, we have seen highly sophisticated malware used to sabotage the business activities of chosen targets. We have seen malware such as W32.Stuxnet designed to tamper with industrial automation systems and other destructive examples such as W32.Disstrack and W32.Flamer, which can both wiped out data and files from hard disks. All of these threats can badly disrupt the activities of those affected.

Following along that theme, we recently came across an interesting threat that has another method of causing chaos, this time, by targeting and modifying corporate databases. We detect this threat as W32.Narilam.

Based on the detections observed, W32.Narilam is active predominantly in the Middle East.

Figure 1. *Distribution of W32.Narilam*

Just like many other worms that we have seen in the past, the threat copies itself to the infected machine, adds registry keys, and spreads through removable drives and network shares. It is even written using Delphi, which is a language that is used to create a lot of other malware threats. All these aspects of this threat are normal enough, what is unusual about this threat is the fact that it has the functionality to update a Microsoft SQL database if it is accessible by OLEDB. The worm specifically targets SQL databases with three distinct names: alim, maliran, and shahd.

The following are some of the object/table names that can be accessed by the threat:

- Hesabjari ("current account" in Arabic/Persian).
- Holiday
- Holiday_1
- Holiday_2
- Asnad (“financial bond” in Arabic)
- A_sellers

- A_TranSanj
- R_DetailFactoreForosh ("forosh" means "sale" in Persian)
- person
- pasandaz ("savings" in Persian)
- BankCheck
- End_Hesab ("hesab" means "account" in Persian)
- Kalabuy
- Kalasales
- REFcheck
- buyername
- Vamghest (“instalment loans” in Persian)

The threat replaces certain items in the database with random values. The following are some of the items that are modified by the threat:

- Asnad.SanadNo ("sanad" means "document" in Persian)
- Asnad.LastNo
- Asnad.FirstNo
- A_TranSanj.Tranid
- Pasandaz.Code (“pasandaz” means “savings” in Persian)
- n_dar_par.price
- bankcheck.state
- End_Hesab.Az
- Kalabuy.Serial
- sath.lengths
- Kalasales.Serial
- refcheck.amount
- buyername.Buyername

The threat also deletes tables including ones with the following names:

- A_Sellers
- person
- Kalamast

Below is a fraction of the temporal procedure that is specified in the threat code.

Figure 2. *Code snippet showing an extract of the temporal procedure*

For example, in line 12 through 14, it sets a variable, @SanadNo, to a value that is randomly chosen between zero and the maximal value in Koll.Koll records. Then it deletes a record in Koll table where the Koll.Koll value is the same as the random value.

The malware does not have any functionality to steal information from the infected system and appears to be programmed specifically to damage the data held within the targeted database. Given the types of objects that the threat searches for, the targeted databases seem to be related to ordering, accounting, or customer management systems belonging to corporations.

Our in-field telemetry indicates that the vast majority of users impacted by this threat are corporate users. This fact is consistent with the functionality contained within the threat. The types of databases that this threat is looking for is unlikely to be found in the systems of home users.

Figure 3.*Narilam infections broken down by user type*

Unless appropriate backups are in place, the affected database will be difficult to restore. The affected organization will likely suffer significant disruption and even financial loss while restoring the database. As the malware is aimed at sabotaging the affected database and does not make a copy of the original database first, those affected by this threat will have a long road to recovery ahead of them.

Symantec users with the latest definitions are protected from W32.Narilam; however, we strongly recommend that important databases be backed up regularly.