SECURELIST

Narilam: A 'New' Destructive Malware Used In the Middle East

0.6

GReAT
Kaspersky Lab Expert
Posted November 26, 11:59 GMT
Tags: Microsoft Windows, Duqu, Targeted Attacks, Stuxnet, Gauss, Flame

Several days ago, our colleagues from Symantec published an analysis of a new destructive malware reported in the Middle East. Dubbed "Narilam", the malware appears to be designed to corrupt databases. The database structure naming indicates that targets are probably in Iran.

We have identified several samples related to this threat. All of them are ~1.5MB Windows PE executables, compiled with Borland C++ Builder. If we are to trust the compilation headers, they appear to have been created in 2009-2010, which means it might have been in the wild for a while:

Count of sections	8	Machine	intel386
Symbol table	00000000[00000000]		Thu Sep 03 19:21:05 2009
Size of optional header	00E0	Magic optional header	010B
Linker version	5.00	OS version	4.00
Image version	0.00	Subsystem version	4.00
Entry point	00001410	Size of code	000C6000
Size of init data	00092000	Size of uninit data	00000000
Size of image	00198000	Size of header	00000600
Base of code	00001000	Base of data	000C7000
Image base	00400000	Subsystem	Windows GUI
Section alignment	00001000	File alignment	00000200
Stack	00100000/00002000	Heap	00100000/00001000
Checksum	00198EB2	Number of directories	16

The earliest known sample has a timestamp of "**Thu Sep 03 19:21:05 2009**".

According to Kaspersky Security Network, there are very few reports of this malware at the moment, which means it's probably almost extinct. The earliest report of the malware is from August 2010; in total about 80 incidents have been recorded during past two years.

Several versions of this Trojan are detected by Kaspersky products as **Trojan.Win32.Scar.cvcw** and **Trojan.Win32.Scar.dlvc**. Some newer versions of the malware are detected heuristically by Kaspersky products, as **HEUR:Trojan.Win32.Generic**.

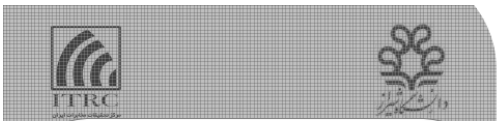
Similarities with Wiper, Stuxnet, Duqu or Flame

According to some reports, the malware could be related to a chain of attacks which have targeted Iran during the past two years, and which our readers are probably aware of.

We've analyzed the sample and found no obvious connection with these. Duqu, Stuxnet, Flame and Gauss have all been compiled with versions of Microsoft Visual C, while Narilam was built with Borland C++ Builder 6 (and not Delphi, as other articles seem to suggest), a completely different programming tool.

How old is it really?

As usual, compilation timestamps can be faked, so we were wondering if we could find other proof of this malware being ItW for a while. We were indeed able to find a CERT alert from June 2010 which appears to relate to this malware.




مرکز تخصصی آپا درزمینه اختلالات امنیتی مرتبط با بد افزارها

cert@shirazu.ac.ir

Win32/Trojan Agent.akk

تنظیم کننده:

علیرضا سبحانی

ویرایش: ۱

شماره سند: V-89/9-5

www.ircert.cc

The alert references a malware with slightly different size, but the same payload: *"The malware changes in the database tables, integrated systems Amin, Maliran, Shahd"*. An alternative name for it is "Trojan.AKK".

In addition to this, yesterday (Sunday Nov 25th, 2012) the Iranian Maher CERT team published an alert about the malware in which they say it was *'previously detected and reported online in 2010'*.

Targeted software

As mentioned in Symantec's report, the malware appears to target databases with some very specific names: maliran, shahd and amin. It works by randomly deleting records from several tables named "A_Sellers", "Koll" or "Moein":

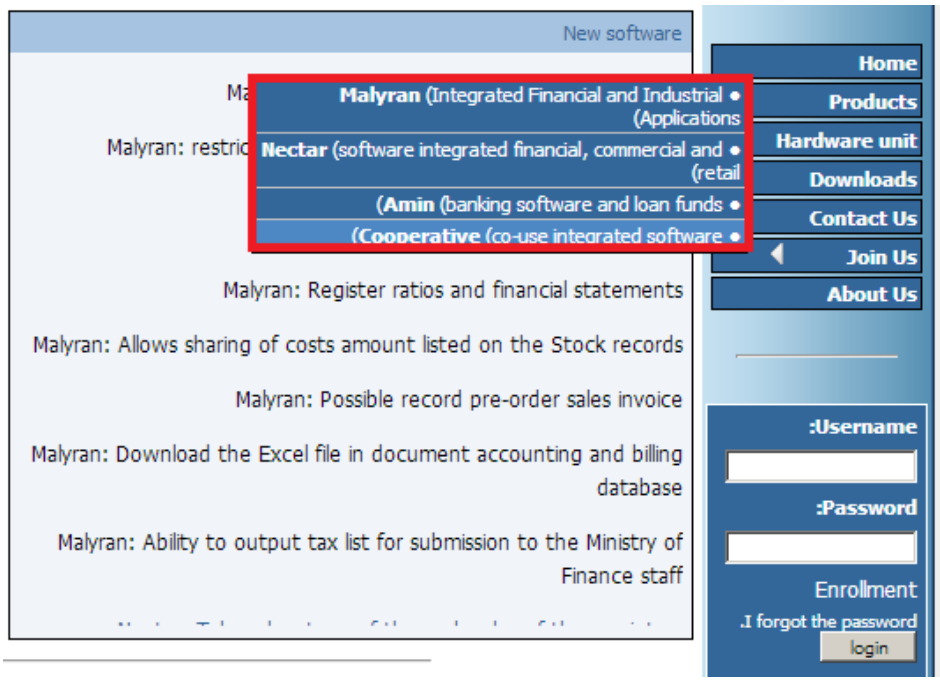
```
delete from A_Sellers Where Cast(sellercod as int)=@SanadNo
delete from Koll Where Cast(Koll as int)=@SanadNo
delete from Moein Where Cast(Moein as int)=@SanadNo
delete from Tafsily Where Cast(Tafsily as int)=@SanadNo
delete from person Where Cast(code as int)=@SanadNo
delete from Vamghest  Where Cast(vamno as int)=@vamno and @dresid=dresid
delete from Kalamast Where Idx =@SanadNo
```

Could these be specific to a certain company or software used by the targeted companies?

Earlier today, an Iranian company named "TarrahSystem" put out an alert about "W32.Narilam" targeting some of their software:

A rough translation of the alert recommends users to “prepare backups” because of new malware (W32.Narilam) targeting “financial software”.

Both “maliran” and “amin” appear to be products from TarrahSystem:



- **Maliran** – Integrated Financial and Industrial Applications
- **Amin** – Banking and Loans Software
- **Shahd** (“Nectar”) – Integrated Financial / Commercial Software

Could it be that “Narilam” targets these 3 products from TarrahSystem? Unfortunately, we do not have these three programs to check, but it’s quite likely.

Summary and conclusions

Considering compilation timestamps and early reports, Narilam is a rather old threat that was probably deployed during late 2009 and mid-2010. Its purpose was to corrupt databases of three financial applications from TarrahSystem, namely Maliran, Amin and Shahd. Several variants appear to have been created, but all of them have the same functionality and method of replication.

Reports from Kaspersky Security Network indicate that the malware was found mostly in Iran (~60%) and Afghanistan (~40%).

At the moment, we do not see any direct connection with other recent destructive malware (such as Shamoon or Wiper). Unlike Duqu or Flame, there is no apparent cyberespionage function.

The malware is currently almost extinct – during the past month, we have observed just six instances of this threat.

We will continue to monitor the situation and update this post as needed.