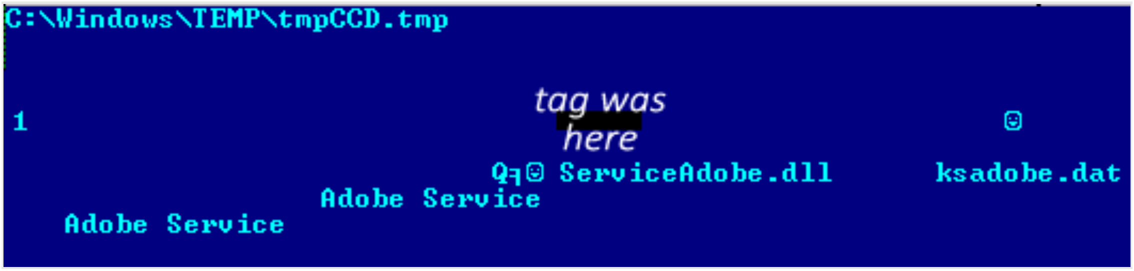
Games are over: Winnti is now targeting pharmaceutical companies

For a long time the Winnti group had been considered as a Chinese threat actor targeting gaming companies specifically. Recently, we've seen information indicating that the scope of targets can be wider and is no longer limited to the entertainment business. We actually track samples of Winnti malware all the time, but so far we haven't been able to catch one with solid clues indicating other targeted industries. Also our visibility as a vendor does not cover every company in the world (at least so far ;)) and the Kaspersky Security Network (KSN) did not reveal other attacks except those against gaming companies. Well, sometimes targeted entities have included telecommunication companies, or better, large holdings, but it seems that at least one of their businesses was in some way related to the production or distribution of computer games.

In April Novetta released its excellent report on the Winnti malware spotted in the operations of Axiom group. The Axiom group has been presented as an advanced Chinese threat actor carrying out cyber-espionage attacks against a whole range of different industries. For us, the Novetta report was another source of intelligence that Winnti was already expanding beyond online games. One of the recent Winnti samples we found appears to confirm this as well.

The new sample belongs to one of the Winnti versions described in Novetta's report – Winnti 3.0. This is one of the Dynamic Link Libraries composing this RAT (Remote Access Trojan) platform – the worker library (which in essence is the RAT DLL) with the internal name *w64.dll* and the exported functions *work_end* and *work_start*. Since, as usual, this component is stored on the disk with the strings and much of other data in the PE header removed/zeroed, it is impossible to restore the compilation date of this DLL. But this library includes two drivers compiled on August 22 and September 4, 2014. The sample has an encrypted configuration block placed in overlay. This block may include a tag for the sample – usually it is a campaign ID or victim ID/name. This time the operators put such tag in the configuration and it turned out to be the name of the **well-known global pharmaceutical company headquartered in Europe**:



```
C:\Windows\TEMP\tmpCCD.tmp

 1                                    tag was                          ☺
                                       here [redacted]
                           Q╕☺ ServiceAdobe.dll        ksadobe.dat
                    Adobe Service
    Adobe Service
```

Pic.1 Configuration block

Besides the sample tag, the configuration block includes the names of other files involved in the working of the RAT platform and the service name (*Adobe Service*), after which malware is installed. The presence of the following files could indicate that the system has been compromised:

C:\Windows\TEMP\tmpCCD.tmp
ServiceAdobe.dll
ksadobe.dat

One of the mentioned drivers (a known, malicious Winnti network rootkit) was **signed with a stolen certificate of a division of a huge Japanese conglomerate**. Although this division is involved in microelectronics manufacturing, other business directions of the conglomerate include **development and production of drugs as well as medical equipment**.

Although the nature of the involvement of Winnti operators, who were earlier perceived to be a threat only to the online gaming industry, in the activities of other cyber-espionage teams still remains rather obscure, the evidence is there. From now on, when you see Winnti mentioned, don't think just about gaming companies; consider also at least targeted telecoms and big pharma companies.

Here are the samples in question:

8e61219b18d36748ce956099277cc29b – Backdoor.Win64.Winnti.gy
5979cf5018c03be2524b87b7dda64a1a – Backdoor.Win64.Winnti.gf
ac9b247691b1036a1cdb4aaf37bea97f – Rootkit.Win64.Winnti.ai