New wiper malware discovered by Kaspersky

Kaspersky Lab's Global Research and Analysis Team has discovered a new sophisticated wiper malware similar to Shamoon.

In 2012, the Shamoon (also known as Disttrack) wiper took down roughly 35,000 computers in an oil and gas company in the Middle East. This attack left 10% of the world's oil supply potentially at risk. However, the incident was one of a kind, and after it the actor essentially went dark. In late 2016 it returned in the form of Shamoon 2.0 – a far more extensive malicious campaign using a heavily updated version of the 2012 malware.

While exploring these attacks Kaspersky Lab researchers unexpectedly found malware that was built in a similar "style" to Shamoon 2.0. At the same time, it was very different and more sophisticated than Shamoon. They named it StoneDrill.

StoneDrill also features advanced anti-detection techniques and espionage tools in its arsenal. In addition to targets in the Middle East, one target has also been discovered in Europe, where wipers used in the Middle East have not previously been spotted in the wild.

StoneDrill – a wiper with connections

It is not yet known how StoneDrill is propagated, but once on the attacked machine it injects itself into the memory process of the user's preferred browser. During this process, it uses two sophisticated anti-emulation techniques aimed at fooling security solutions installed on the victim machine. The malware then starts destroying the computer's disk files.

click to enlarge

So far, at least two targets of the StoneDrill wiper have been identified, one based in the Middle East and the other in Europe.

Besides the wiping module, Kaspersky Lab researchers have also found a StoneDrill backdoor, which has apparently been developed by the same code writers and used for espionage purposes. Experts discovered four command and control panels which were used by attackers to run espionage operations with help of the StoneDrill backdoor against an unknown number of targets.

Perhaps the most interesting thing about StoneDrill is that it appears to have connections to several other wipers and espionage operations observed previously. When Kaspersky Lab researchers discovered StoneDrill with the help of Yara-rules created to identify unknown samples of Shamoon, they realised they were looking at a unique piece of malicious code that seems to have been created separately from Shamoon. Even though the two families – Shamoon and StoneDrill – don't share the exact same code base, the mind-set of the authors and their programming "style" appear to be similar. That's why it was possible to identify StoneDrill with the Shamoon-developed Yara-rules.

Code similarities

Code similarities with older known malware were also observed. StoneDrill uses some parts of the code previously spotted in the NewsBeef APT, also known as Charming Kitten – another malicious campaign which has been active in the last few years.

"We were very intrigued by the similarities and comparisons between these three malicious operations. Was StoneDrill another wiper deployed by the Shamoon actor? Or are StoneDrill and Shamoon two different and unconnected groups that just happened to target Saudi organisations at the same time? Or, two groups which are separate but aligned in their objectives?

"The latter theory is the most likely one: when it comes to artefacts we can say that while Shamoon embeds Arabic-Yemen resource language sections, StoneDrill embeds mostly Persian resource language sections. Geopolitical analysts would probably be quick to point out that both Iran and Yemen are players in the Iran-Saudi Arabia proxy conflict, and Saudi Arabia is the country where most victims of these operations were found. But of course, we do not exclude the possibility of these artefacts being false flags," said Mohamad Amin Hasbini, senior security researcher, Global Research and Analysis Team, Kaspersky Lab.

Protection

- Conduct a security assessment of the control network (i.e. a security audit, penetration testing, gap analysis) to identify and remove any security loopholes. Review external vendor and third party security policies in case they have direct access to the control network.
- Request external intelligence: intelligence from reputable vendors helps organisations to predict future attacks on the company's industrial infrastructure.
- Train your employees, paying special attention to operational and engineering staff and their awareness of recent threats and attacks.
- Provide protection inside and outside the perimeter. A proper security strategy has to devote significant resources to attack detection and response in order to block an attack before it reaches critically important objects.

- Evaluate advanced methods of protection including regular integrity checks for controllers, and specialised network monitoring to increase the overall security of a company and reduce the chances of a successful breach, even if some inherently vulnerable nodes cannot be patched or removed.