Shamoon: Back from the dead and destructive as ever

4 Recommend

Nov 30, 2016 11:53 AM

A L Johnson

Shamoon (W32.Disttrack), the aggressive disk-wiping malware which was used in attacks against the Saudi energy sector in 2012, has made a surprise comeback and was used in a fresh wave of attacks against targets in Saudi Arabia.

The malware used in the recent attacks (W32.Disttrack.B) is largely unchanged from the variant used four years ago. In the 2012 attacks, infected computers had their master boot records wiped and replaced with an image of a burning US flag. The latest attacks instead used a photo of the body of Alan Kurdi, the three year-old Syrian refugee who drowned in the Mediterranean last year.

Carefully planned operation

The attackers appear to have done a significant amount of preparatory work for the operation. The malware was configured with passwords that appear to have been stolen from the targeted organizations and were likely used to allow the threat to spread across a targeted organization's network. How the attackers obtained the stolen credentials is unknown.

The malware had a default configuration that triggered the disk-wiping payload at 8:45pm local time on Thursday, November 17. The Saudi Arabian working week runs from Sunday to Thursday. It would appear that the attack was timed to occur after most staff had gone

home for the weekend in the hope of reducing the chance of discovery before maximum damage could be caused.

How Shamoon works

Shamoon uses a number of components to infect computers. The first component is a dropper, which creates a service with the name 'NtsSrv' to remain persistent on the infected computer. It spreads across a local network by copying itself on to other computers and will drop additional components to infected computers. The dropper comes in 32-bit and 64-bit versions. If the 32-bit dropper detects a 64-bit architecture, it will drop the 64-bit version.

The second component is the wiper, which drops a third component, known as the Eldos driver. This enables access to the hard disk directly from user-mode without the need of Windows APIs. The wiper uses the Eldos driver to overwrite the hard disk with the aforementioned photos of the Syrian boy.

The final component is the reporter. This is responsible for handling communications with a command and control (C&C) server operated by the attackers. It can download additional binaries from the C&C server and change the pre-configured disk-wiping time if instructed by the C&C server. It is also configured to send a report verifying that a disk has been wiped to the C&C server.

Back with a bang

Although attacks involving destructive malware such as Shamoon are relatively rare, they can be highly disruptive for the targeted organization, potentially knocking mission-critical computers offline.

Why Shamoon has suddenly returned again after four years is unknown. However, with its highly destructive payload, it is clear that the attackers want their targets to sit up and take notice.

Protection

Symantec and Norton products protect against Shamoon with the following detections:

Antivirus

Intrusion prevention system

Statistics

0 Favorited

1 Views

0 Files

0 Shares

0 Downloads

Tags and Keywords

Related Entries and Links

No Related Resource entered.