Greenbug cyberespionage group targeting Middle East, possible links to Shamoon

By By

Published: 2017-01-23 · Archived: 2026-04-05 14:27:59 UTC

Symantec is currently investigating reports of yet another new attack in the Middle East involving the destructive disk-wiping malware used by the Shamoon group (W32.Disttrack, W32.Disttrack.B). Similar to previous attacks, the Disttrack malware used by Shamoon is just the destructive payload. It required other means to be deployed on targeted organizations' networks and is configured with previously stolen credentials.

Symantec discovered the Greenbug cyberespionage group during its investigation into previous attacks involving W32.Disttrack.B (aka Shamoon). Shamoon (W32.Disttrack) first made headlines in 2012 when it was used in attacks against energy companies in Saudi Arabia. It recently resurfaced in November 2016 (W32.Disttrack.B), again attacking targets in Saudi Arabia. While these attacks were covered extensively in the media, how the attackers stole these credentials and introduced W32.Disttrack on targeted organizations' networks remains a mystery.

Could Greenbug be responsible for getting Shamoon those stolen credentials?

Greenbug was discovered targeting a range of organizations in the Middle East including companies in the aviation, energy, government, investment, and education sectors. The group uses a custom information-stealing remote access Trojan (RAT) known as Trojan.Ismdoor as well as a selection of hacking tools to steal sensitive credentials from compromised organizations.

Although there is no definitive link between Greenbug and Shamoon, the group compromised at least one administrator computer within a Shamoon-targeted organization's network prior to W32.Disttrack.B being deployed on November 17, 2016.

Is there a link between Greenbug and the disk-wiping Shamoon attacks?

Attack analysis

Active since at least June 2016, Greenbug most likely uses email to compromise targeted organizations. Symantec believes the group has exclusive access to the malware Trojan.Ismdoor. The group uses additional tools to compromise other computers on the network and steal user names and passwords from operating systems, email accounts, and web browsers.

Between June and November 2016, Trojan.Ismdoor was used against a number of targets in a wide range of sectors across the Middle East. As part of the operation, legitimate infrastructure belonging to an organization in the energy sector was used to host the Ismdoor payload. Attacks impacted organizations involved in aviation,

government, investment, and education. Additional regions affected include Saudi Arabia, Iran, Bahrain, Iraq, Qatar, Kuwait, and Turkey. A Saudi organization in Australia was also targeted.

It is believed that the attacks start with an email that asks the recipient to download a RAR archive containing what is purported to be information about a business proposal. These lure documents were hosted on a legitimate website, which may have been previously compromised by Greenbug. The Ismdoor malware is hidden inside the RAR archive using an alternate data stream.

Windows Alternate Data Streams (ADS) is a feature of NTFS which is used to store details about a file. The information stored in ADS is hidden to the user, which makes it an attractive feature for attackers. ADS is sometimes abused by attackers to hide malware or other hacking tools on a compromised computer.

Trojan.Ismdoor

The downloaded RAR archive contains three components including a .pdf file and a .chm (Compiled HTML Help) file, which includes an ADS hiding the payload (Trojan.Ismdoor). The clean .pdf file contains instructions on how to open the .chm file. Opening the .chm file, which includes the malicious ADS, will execute the Ismdoor Trojan.

Once executed, Trojan.Ismdoor opens a back door on the compromised computer, leveraging Windows PowerShell for command and control. The Trojan then has the ability to install other malware as well as collect system data from infected computers that it can use to determine which additional tools to deploy for further data collection.

Greenbug has been observed downloading a number of tools used to log keystrokes and collect browser, email, and other sensitive data such as user credentials.

Is Greenbug responsible for delivering Shamoon?

The presence of Greenbug within an organization prior to the destructive attack involving W32.Disttrack.B provides only a tentative connection to Shamoon. Greenbug's choice of targets and the fact that Ismdoor and associated tools downloaded by the threat appear to have gone quiet a day prior to the November 17, 2016 Shamoon attack is, however, suspicious. At this time, Symantec tracks these groups separately unless additional corroborating evidence emerges.

Symantec is currently investigating reports of new Shamoon activity in the Middle East. Whether or not evidence of Greenbug activity will be discovered during the investigation remains to be seen. However, one thing is clear, destructive attacks carried out by Shamoon are still a dangerous reality facing organizations in the Middle East.

Protection

Symantec and Norton products protect against the threats discussed in this blog with the following detections:

Greenbug

Antivirus

- Trojan.Ismdoor
- Trojan.Ismdoor!gen1

Intrusion prevention system

- System Infected: Trojan.Ismdoor Activity

Shamoon

Antivirus

- W32.Disttrack
- W32.Disttrack!gen1
- W32.Disttrack!gen4
- W32.Disttrack!gen6
- W32.Disttrack!gen7
- W32.Disttrack!gen8
- W32.Disttrack.B
- PUA.Disttrack!sys

Intrusion prevention system

- System Infected: Disttrack Trojan Activity 2
- System Infected: Disttrack Trojan Activity 3
