Shamoon Collaborator Greenbug Adopts New Communication Tool

By Tom Spring

Published: 2017-05-02 · Archived: 2026-04-05 14:21:22 UTC

New clues surface on Shamoon's ability steal credentials ahead of attacks.

Researchers have identified a possible new collaborator in the continued Shamoon attacks against Saudi organizations. Called Greenbug, this group is believed to be instrumental in helping Shamoon steal user credentials of targets ahead of Shamoon's destructive attacks.

However, researchers know about as much about Greenbug as they do Shamoon; which isn't much. But, that's slowly changing.

On Tuesday, Arbor Networks said that it has new leads on a credential stealing remote access Trojan (RAT) called Ismdoor, possibly used by Greenbug to steal credentials on Shamoon's behalf.

"With our latest research we now see how Greenbug has shifted away from HTTP-based C2 communication with Ismdoor. It's now relying on a new DNS-based attack technique to better cloak command and control communications between Greenbug and the malware," said Dennis Schwarz, research analyst on Arbor's ASERT Team, in an interview with Threatpost.

He said Greenbug is using DNS TXT record queries and responses to create a bidirectional command and control channel.

"One major change in recent versions (of Ismdoor) has been the replacement of the old HTTP based command and control functionality with a custom covert channel using AAAA DNS queries for IPv6 addresses," Schwarz wrote in a technical analysis of the malware posted Monday.

Using the DNS attack technique, adversaries can use DNS communications to submit commands to be run on systems infected with the Ismdoor RAT. Schwarz said using this technique, data is also be exfiltrated from the machines as well. "This is an extremely rare and covert way to administer a RAT," he said.

DNS tunneling takes advantage of the TXT transport layer within the DNS protocol used by top- and second-level domain name system servers. A maximum of 255 bytes of data can be transported via DNS requests between endpoint and a DNS server using the TXT layer. For attackers that have already gained a foothold on targeted systems, the DNS tunneling of commands and DNS tunneling used to remove data is extremely slow, but well suited for long term APT campaigns.

"All data sent between the bot and the C2 is done using AAAA DNS UDP queries. Data to the C2 is via specially crafted query names and data from the C2 is returned via IPv6 addresses. The bot side of the connection drives all communications," according to Schwarz's analysis.

Use of DNS-based message attacks has been used in similar attacks documented by Cisco Talos where adversaries use DNS queries to carry out malicious PowerShell commands on compromised computers. Last year, Palo Alto Networks reported a shift in malware tactics used by the APT group Wekby that utilized the DNS TXT transport layer. Cisco calls these types of attacks DNSMessenger attacks. Palo Alto Networks calls them DNS tunneling attacks.

In the context of the Ismdoor RAT, the DNS attack technique is used primarily by Greenbug for stealing credentials. To do this, it employs a number of specific commands via DNSMessenger. One is “CreateMimi1Bat”; which likely executes Mimikatz (executes PowerShell scripts: ccd61.ps1 and Invoke-bypassuac), according to Arbor. Another command is “ExecuteKL”; which likely executes a keylogger (executes Winit.exe and sends “Start Keylog Done” message back to the C2), according to Arbor.

“The threat group that could be behind the original Shamoon attacks is still alive and well. They are definitely advancing the malware. While this DNS form of communication is not new, it’s far from a copy-and-paste type attack. This type of attack takes a dedicated programmer to think it through and put it together,” Schwarz said.
