APT15 Pokes Its Head Out With Upgraded MirageFox RAT

This is the first evidence of the China-linked threat actor's activity since hacked the U.K. government and military in 2017 (which wasn't made public until 2018).

Author: Tara Seals

5:58 pm

2 minute read

The elusive APT15 cyber-espionage group, believed to be affiliated with the Chinese government, has been spotted for the first time in many months, mounting a highly targeted spy campaign using an upgraded version of the Mirage remote access trojan.

This is the first evidence of the China-linked actor's activity since hacking the U.K. government and military in 2017 (which wasn't made public until 2018).

The effort follows the known APT15 pattern of infiltrating specific targets with basic tools that are then customized to carry out tailored data exfiltration once the victim has been breached. The victim organization in this instance has not been made public, according to a technical analysis of APT15 published by researchers at Intezer last Thursday.

A New and Improved RAT

The updated version of the Mirage RAT is called MirageFox. This new version of the RAT was discovered in early June by Intezer, which recognized a specific signature based off code only found in the earlier version of Mirage – and loosely related malware called Reaver. The MirageFox signature was a new upload to VirusTotal, with very few detections.

"MirageFox is very similar to APT15's old RAT, Mirage, but was upgraded to be undetected by most antivirus, and was tailor-made for their target (meaning they had already breached their target, done reconnaissance work and made this version of the RAT to work specifically in that environment)," Jay Rosenberg, senior researcher at Intezer, explained to Threatpost in an interview. "The RAT uses a hard-coded, internal network IP address as the C&C. This means they already have a node inside the internal network to exfiltrate the stolen data."

Mirage is an aging RAT at this point, Rosenberg noted.

"Over the weekend, I discovered that the first version of the RAT Mirage was uploaded to VirusTotal in 2009, meaning that the previously believed information that the APT15 was active since 2010 and Mirage originated in 2012 are wrong," he said.

Malware Code Retread

The upgraded version of the malware is an example of code reuse with a few new bells and whistles, researchers said.

The remote shell function used for executing commands and the function for decrypting the data containing the C&C configuration are recycled from the previous version of Mirage, for instance. It also performs the same functions, i.e. collecting information about the computer like the username, CPU information, architecture and so forth before opening a backdoor and awaiting orders for modifying files, gathering data, launching processes and terminating itself, among other things. The C&C commands are sent manually, the analysis found.

In terms of interesting fresh functions, looking at an unusual export feature, there appears to be "some type of DLL hijacking going on," carried out by distributing a legitimate McAfee binary in a bid to look trustworthy. DLL hijacking techniques have been seen in the past with the APT15 group, Rosenberg said.

Curiously, there's no persistence in the module—it renames itself so that future executions of the RAT will not be through a McAfee binary – perhaps because APT15 already has taken root in the target networks making re-execution moot.

"The future persistence could be setup through another component of the malware or even a command sent by the C&C to the infected computer," Rosenberg said in the analysis.

The decrypted C&C configuration in MirageFox is notable too, he added; the IP address being used for the C&C is actually an internal IP address on the victim company's network. Rosenberg said this likely indicates that the malefactors stole a VPN private key in order to breach the organization. Other details on the threat vector are not known.

A Rarely-Seen Threat Group

The China-linked APT15 (a.k.a. Vixen Panda, Ke3chang, Royal APT or Playful Dragon) is a seldom-seen threat actor, although Rosenberg believes the group is always busy without coming to the attention of researchers.

"I believe APT15's campaigns are ongoing all the time," he told Threatpost. "It's only from time-to-time that an incident comes out to the public, because [victim] organizations or companies do not want the public to know that they were breached."

As for companies and organizations protecting themselves, "it is very difficult because the tools used are very basic and customized once the target has been infiltrated," Rosenberg said in the interview. "For example, once they have infiltrated an organization, they can see if an AV product is installed, and test to make sure everything is undetected by that AV in their own environment before deploying another part of their toolset."

The types of companies and organizations they go after are typical nation-state targets, including government, military, contractors, the oil industry and others.

"Basically, [they attack] anyone they could target that would gather some type of intelligence," Rosenberg told us. "This is the first evidence of their activity since they hacked the U.K. government and military in 2017." That effort used multiple customized backdoors installed on a UK government contractor's computer systems; information about the hack was not made public until March 2018 however, by NCC Group.

Featured | Hacks | Malware

INFOSEC INSIDER

A Practical Guide to Zero-Trust Security
January 22, 2020 2

7 Tips for Maximizing Your SOC
December 31, 2019 5

Mean Time to Hardening: The Next-Gen Security Metric
December 30, 2019 4

Combining AI and Playbooks to Predict Cyberattacks
December 26, 2019 1

The Case for Cyber-Risk Prospectuses
December 24, 2019 1

SUGGESTED ARTICLES

Revamped HawkEye Keylogger Swoops in on Coronavirus Fears

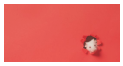
Emails claiming to be directly from WHO's Dr. Tedros Adhanom Ghebreyesus offer "drug advice" — and malware infections.

March 20, 2020

TrickBot Trojan Adds RDP Brute-Forcing to Its Arsenal

A fresh module aims to compromise remote desktop accounts to access corporate resources.

March 18, 2020



APT36 Taps Coronavirus as 'Golden Opportunity' to Spread Crimson RAT

The Pakistani-linked APT has been spotted infecting victims with data exfiltration malware.

March 17, 2020

DISCUSSION