RSAC 2019: New Operation Sharpshooter Data Reveals Higher Complexity, Scope

By Lindsey O'Donnell

Published: 2019-03-04 · Archived: 2026-04-05 14:40:41 UTC

New look at server data behind a previously-identified espionage campaign shows that it has exceeded researchers' expectations in complexity, scope and breadth.

SAN FRANCISCO – An insidious reconnaissance campaign discovered in 2018, dubbed Operation Sharpshooter, is much more widespread than previously thought, researchers said.

Operation Sharpshooter was first disclosed in December 2018, using a never-before-seen implant framework to infiltrate global defense and critical infrastructure players — including nuclear, defense, energy and financial companies.

Operation Sharpshooter's campaign initially appeared to begin Oct. 25 – but in a new research report released at the RSA Conference 2019 this week in San Francisco, researchers with McAfee said that the campaign "is more extensive in complexity, scope and duration of operations."

"The analysis led to identification of multiple previously unknown command-and-control centers, and suggest that Sharpshooter began as early as September 2017, targeted a broader set of organizations, in more industries and countries and is currently ongoing," researchers said on Sunday.

Operation Sharpshooter

The espionage campaign began when a splay of malicious documents were sent to targets via Dropbox. The initial attack vector is a document that contains a weaponized macro. Once downloaded, it places embedded shellcode into the memory of Microsoft Word, which acts as a simple downloader for a second-stage implant.

This next stage runs in memory and gathers intelligence. That second-stage implant is a fully modular backdoor called "Rising Sun" that performs reconnaissance on the victim's network, according to the research.

Notably, Rising Sun uses source code from the Duuzer backdoor, a malware first used in a 2015 campaign targeting the data of South Korean organizations, mainly in manufacturing. Duuzer, which is designed to work with 32-bit and 64-bit Windows versions, opens a back door through which bad actors can gather system information. In this situation, the Rising Sun implant gathers and encrypts data from the victim, and fetches the victim devices' computer name, IP address data, native system information and more.

Widespread Campaign

In December, researchers detected the campaign's implant in 87 organizations worldwide, predominantly in the U.S. (about 50 percent of attacks) and in other English-speaking companies.

However, newly discovered command-and-control server data and code used by the espionage campaign suggests that Sharpshooter began as early as September 2017, targeting a broader set of organizations, and in more industries and countries. That campaign is currently ongoing, researchers said.

The most recent attacks appear to primarily target financial services, government and critical infrastructure, with the largest number taking aim at Germany, Turkey, the United Kingdom and the United States.

The analysis also exposed striking similarities between the technical indicators, techniques and procedures exhibited in the 2018 Sharpshooter attacks, and features of multiple other groups of attacks attributed to the Lazarus Group.

For instance, Rising Sun is similar to the Lazarus Group's Duuzer implant, and source code from the Lazarus Group's infamous 2016 backdoor trojan Duuzer.

"Technical evidence is often not enough to thoroughly understand a cyber attack, as it does not provide all the pieces to the puzzle," said Christiaan Beek, McAfee senior principal engineer and lead scientist. "Access to the adversary's command-and-control server code is a rare opportunity. These systems provide insights into the inner workings of cyberattack infrastructure, are typically seized by law enforcement, and are only rarely made available to private sector researchers."

For all Threatpost's RSA Conference 2019 coverage, please visit our special coverage section, available here.
