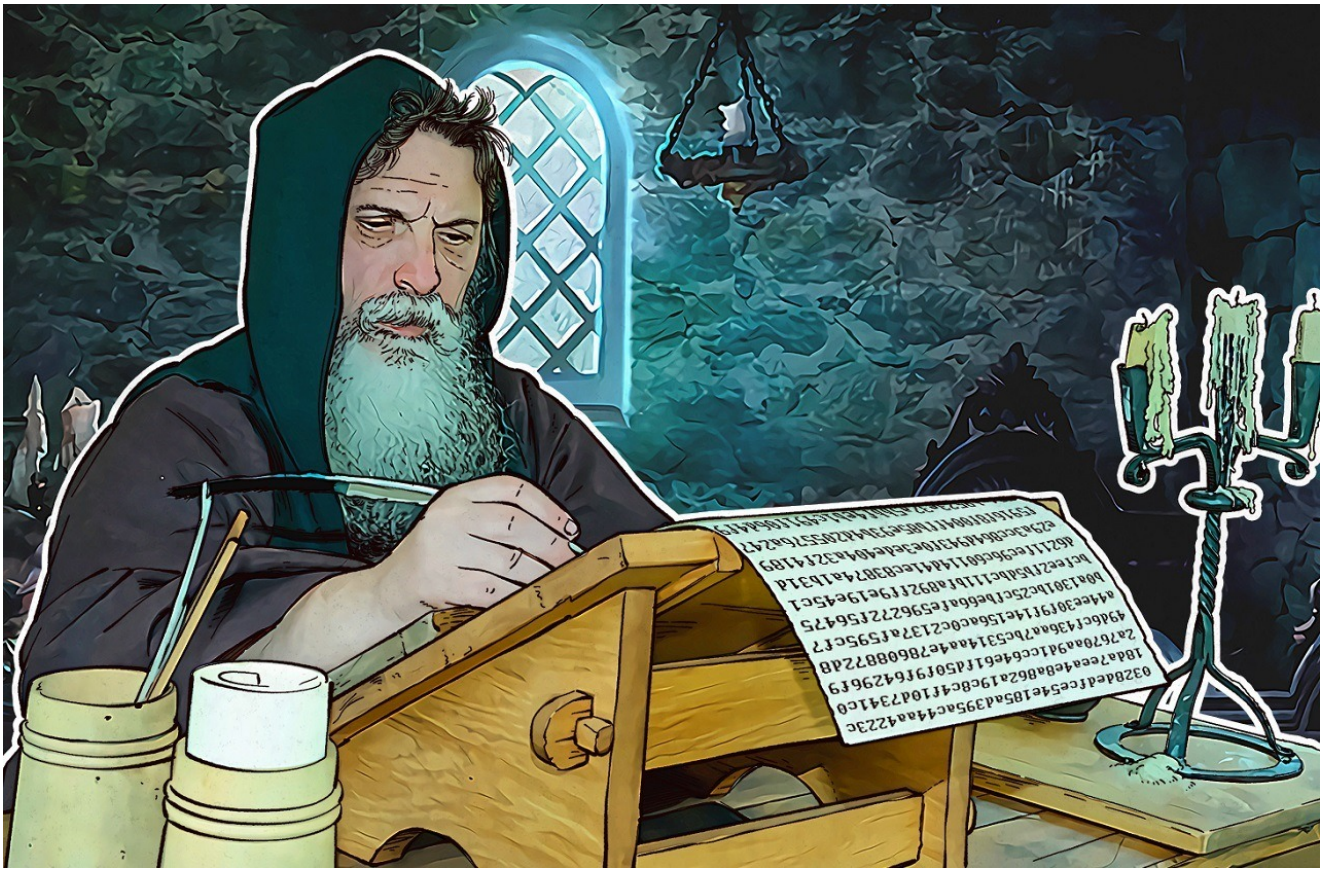
Moonlight Maze: Lessons from history

kaspersky.com/blog/moonlight-maze-the-lessons/6713/

SAS

A possible connection between Moonlight Maze, an APT that targeted the Pentagon and NASA in the late 1990s, and Turla, a modern day threat actor.

- 
  Nikolay Pankov
- April 3, 2017



From the outside, it may seem that the investigation of APT attacks is limited to understanding how the attackers managed to execute their plan and preventing its replication. However, that is not enough. True cybersecurity experts need answers to a wider

range of questions. What was the purpose of the attack? Did attackers succeed? What tools were involved in the attack? Where else were similar methods and programs used?

Answers to these questions help with forecasting the further development of trends, and most important, help with prompt response to future attacks of the same authorship or campaigns that employ the same code. That is why it is important not only to study the mode of action of modern cybercriminals, but also to understand the methods of all earlier attacks. As a company that's been engaged in information security for 20 years, we understand this as few others can.

That is why our experts, aided by researchers from King's College London, have carefully studied Moonlight Maze — one of the first widely known cyberespionage campaigns, active since at least 1996. It is of particular interest because several independent experts from countries have voiced the proposition that it is associated with a much more modern — and still active — group, the authors of the Turla APT attack.

Even the story of how our experts got the information about Moonlight Maze deserves special mention. Initially, in the late nineties, all of the investigation materials were classified by US law enforcement agencies, and so inaccessible to researchers. However, in an attempt to cover their tracks, the attackers used an extensive network of proxy servers working in various universities and libraries in the United States, as well as at least one server in England. On the English server, the local system administrator, who worked on the case with London police and the FBI, activated the logging of all activities. And those logs survived to our times. As a result, our experts got a unique time capsule containing a detailed record of all the attacker's actions.

Watch Video At:

https://youtu.be/9RorL9y70GU

Perhaps the most interesting finding of their research is the backdoor that was used in Moonlight Maze. It was based on the Unix program LOKI2, which was released in 1996 and allowed transmission of data via covert channels. Linux backdoors were also employed in Turla, which Kaspersky Lab first detected in 2014. And those backdoors were built on the basis of LOKI2 as well. Code created more than 20 years ago is still used by modern actors, albeit in a slightly updated form.

You can find a full study on Securelist, along with a brief excursion into the history of this APT (which reads like a good detective story).

The takeaway here is nothing new: You have to know the past to understand the present. Therefore, while conducting investigations of new cyberincidents, our experts call on knowledge accumulated for more than 20 years.

In addition, this story is a good reminder to those who still believe that Linux platforms are inherently safe. They are wrong. And their mistake is already at least 21 years old.

- APT
- Moonlight Maze
- SAS
- SAS 2017
- True Cybersecurity
- Turla

Share article

Related