EARTH BAKU

An APT Group Targeting Indo-Pacific Countries With New Stealth Loaders and Backdoor

Toward the end of 2020, we observed a new cyberespionage campaign that had been carried out since at least July of that year by Earth Baku, the advanced persistent threat (APT) group more widely known as APT41. Our research presents an in-depth study of this campaign, including the ways in which Earth Baku has evolved its malware tools for its attacks.

KEY FINDINGS

Targets in the Indo-Pacific region

The campaign has affected businesses and government agencies in the airline, computer hardware, automotive, infrastructure, publishing, media, and IT industries. These targets are located in countries including India, Indonesia, Malaysia, the Philippines, Taiwan, and Vietnam.

Updated toolset

The campaign uses two new shellcode loaders, which we have named StealthMutant and StealthVector. These loaders are designed with a variety of techniques for evading detection. Their payload is either the Cobalt Strike beacon or a recently discovered shellcode-based backdoor, which we have dubbed ScrambleCross.

Multiple attack vectors

Earth Baku uses various mechanisms to gain access to its targets' networks, including SQL injection into a web application, exploitation of a Microsoft Exchange Server vulnerability, use of an installer application via a scheduled task, and, possibly, use of emails with malicious file attachments.

Members with diverse skills

The complexity of Earth Baku's new tools suggests that the APT group includes members whose specialties lie in low-level programming, software development, and techniques used by red teams.

HOW TO PROTECT NETWORKS FROM CYBERESPIONAGE CAMPAIGNS

Threat actor groups like Earth Baku, which has earned a reputation for using advanced malware, are constantly seeking to enhance their arsenals of tools and tactics. Our research paper provides security recommendations — such as formulating an incident response plan, regularly updating systems, and implementing proactive security solutions — to help organizations draw up a solid defense strategy that can effectively prevent and mitigate the impact of cyberespionage attacks.

Learn more about Earth Baku's cyberespionage campaign in our research paper at https://research.trendmicro.com/earthbaku.

TREND MICRO | research