Beat: Technology

Kaspersky Lab identifies infrastructure of Crouching Yeti

Attacks on industrial companies

Jeddah, 27.04.2018, 23:59 Time

USPA NEWS - Kaspersky Lab has uncovered infrastructure used by the well-known Russian-speaking APT group Crouching Yeti, also known as Energetic Bear, which includes compromised servers across the world. According to the research, numerous servers in different countries were hit since 2016, sometimes in order to gain access to other resources. Others, including those hosting Russian websites, were used as watering holes.

Crouching Yeti is a Russian-speaking advanced persistent threat (APT) group that Kaspersky Lab has been tracking since 2010. It is best known for targeting industrial sectors around the world, with a primary focus on energy facilities, for the main purpose of stealing valuable data from victim systems. One of the techniques the group has been widely using is through watering hole attacks: the attackers injected websites with a link redirecting visitors to a malicious server.
Recently Kaspersky Lab has discovered a number of servers, compromised by the group, belonging to different organizations based in Russia, the U.S., Turkey and European countries, and not limited to industrial companies. According to researchers, they were hit in 2016 and 2017 with different purposes. Thus, besides watering hole, in some cases they were used as intermediaries to conduct attacks on other resources.

In the process of analyzing infected servers, researchers identified numerous websites and servers used by organizations in Russia, U.S., Europe, Asia and Latin America that the attackers had scanned with various tools, possibly to find a server that could be used to establish a foothold for hosting the attackers´ tools and to subsequently develop an attack. Some of the sites scanned may have been of interest to the attackers as candidates for waterhole. The range of websites and servers that captured the attention of the intruders is extensive. Kaspersky Lab researchers found that the attackers had scanned numerous websites of different types, including online stores and services, public organizations, NGOs, manufacturing, etc.
Also, experts found that the group used publicly available malicious tools, designed for analyzing servers, and for seeking out and collecting information. In addition, a modified sshd file with a preinstalled backdoor was discovered. This was used to replace the original file and could be authorized with a “˜master password´.

Crouching Yeti is a notorious Russian-speaking group that has been active for many years and is still successfully targeting industrial organizations through watering hole attacks, among other techniques. Our findings show that the group compromised servers not only for establishing watering holes, but also for further scanning, and they actively used open-sourced tools that made it much harder to identify them afterwards,“⍰ said Vladimir Dashchenko, Head of Vulnerability Research Group at Kaspersky Lab ICS CERT.
“The group´s activities, such as initial data collection, the theft of authentication data, and the scanning of resources, are used to launch further attacks. The diversity of infected servers and scanned resources suggests the group may operate in the interests of the third parties.“⍰ he added.

Kaspersky Lab recommends that organizations implement a comprehensive framework against advanced threats comprising of dedicated security solutions for targeted attack detection and incident response, along with expert services and threat intelligence. As a part of Kaspersky Threat Management and Defense, our anti-targeted attack platform detects an attack at early stages by analyzing suspicious network activity, while Kaspersky EDR brings improved endpoint visibility, investigation capabilities and response automation. These are enhanced with global threat intelligence and Kaspersky Lab´s expert services with specialization in threat hunting and incident response.

Article online:
https://www.uspa24.com/bericht-13268/kaspersky-lab-identifies-infrastructure-of-crouching-yeti.html

Editorial office and responsibility:
V.i.S.d.P. & Sect. 6 MDStV (German Interstate Media Services Agreement): Abdullah Inayat

Exemption from liability:
The publisher shall assume no liability for the accuracy or completeness of the published report and is merely providing space for the submission of and access to third-party content. Liability for the content of a report lies solely with the author of such report. Abdullah Inayat

Editorial program service of General News Agency:
United Press Association, Inc.
3651 Lindell Road, Suite D168
Las Vegas, NV 89103, USA
(702) 943.0321 Local
(702) 943.0233 Facsimile
info@unitedpressassociation.org
info@gna24.com
www.gna24.com