Date: 20.4.2022	**Publication:** Mint
Page no.: 5	**Edition:** Kolkata| Ahmedabad |Bangalore |Mumbai| New Delhi ||Hyderabad |

Hackers are targeting machine identities to steal passwords, user info

Sohini Bagchi &
Moumita Deb Choudhury

NEW DELHI

TECHCIRCLE

With companies accelerating adoption of Internet of Things (IoT) and connected devices, and cloud apps, to accommodate remote work during the pandemic, machine identities emerged as the weak link, with increasing instances of cyberattacks leveraging the digital certificates.

For instance, in February, Lapsus launched a cyberattack into chipmaker Nvidia's internal systems and leaked its code-signing certificate online, which was then used by other hackers to bypass authentication protocols used by Windows Defender, a security tool built into all versions of the Windows operating system.

Gaming major Epic Games and certificate authority Let's Encrypt also suffered similar attacks in April 2022 and September 2021, respectively.

Just as human identities are protected with usernames and passwords to authenticate access, machine identities are protected by certificates. With increasing covid-led dependence on communication over connected devices, the number of machine identities have also surpassed human identities.

As a result, hackers are targeting machine identities to steal passwords and user information by breaching a company's internal systems. In fact, security firm CyberArk said in a recent report that machine identities now outweigh human identities by a factor of 45 times. If these digital identities go unmanaged and are not secure, it could lead to the creation of many separate identities that are incompatible with each other, and can create "significant" cybersecurity risk, said Prateek Bhajanka, cybersecurity expert and vice president, products, of American security testing firm Breachlock. "Identities from any machine can be stolen when the host is compromised. Say, in the case of IoT devices, when compromised, its identity can be stolen and when the access rights to the database is abused, it can lead to data exfiltration."

With digital transformation initiatives like cloud migration, the need for machine identities has grown exponentially. ISTOCK

K.V. Dipu, head of operations and customer service at Bajaj Allianz General Insurance expressed similar views. "With digital transformation initiatives like cloud migration and expanding DevOps processes, the need for machine identities has grown exponentially. Enterprises that fail to keep up with the volume and variety of machine identities may end up with serious consequences like data breaches, outages, and much more," he said.

CYBER THREAT

MACHINE identities now outweigh human identities by a factor of 45 times

IF digital identities go unmanaged and are not secure, it can create significant cybersecurity risk

"To avoid a hack, we ensure access permissions are given on a need-to-know basis with permission only to authorized users." Dipu said permissions are granted following strong successful authentication controls. "We also control breach by disallowing all communication channels that are not required," he said.

A recent report by machine identity management firm Venafi said the average number of machine identities per organization reached nearly 250,000 at the end of 2021, up by 42% from 2020.

"The unfortunate reality is that most organizations are not prepared to manage all the machine identities they need," said Kavin Bocek, vice president, security strategy and threat intelligence, Venafi. "This rapidly growing gap has opened a new attack surface—from software build pipelines to kubernetes clusters—and that is very attractive to hackers," he said.

Bocek said while an average organization will have more than 500,000 machines by 2024, the problem is IT teams use "multiple disconnected and manual tools" to track digital certificates.

"There are a number of ways to secure machine identities," said Mary Ruddy, vice president analyst at research firm Gartner. She said enterprises must offer adequate guidance to developers, security and DevOps teams by defining how the various tools in their technology stacks should or should not be used, and under what circumstances new tools or instances can be deployed.