VENAFI®

Malware Exploiting Machine Identities Doubled Between 2018 to 2019

8X increase in malware attacks weaponizing machine identities over the last decade

"Machine identities are increasingly being used in more common attack vectors. Commoditized "off-the-shelf" malware has become more sophisticated and the inclusion of machine identity components makes it much harder to detect. These are massive campaigns, with computer farms, so companies can lose a lot of money or have their resources hijacked if they fall victim; not to mention the damage to their reputation should customer data be put at risk."

Machines use TLS certificates and SSH keys to authenticate themselves and authorize secure connection and communication

More than
31 billion
IoT devices wordwide.[1]

12.3 billion
mobile-connected devices by 2022, including machine-to-machine modules.[2]

500 million
new logical apps will be created between 2018-2023 – equal to the number built over the past 40 years.[3]

The devastating effects of poorly protected machine identities

We could eliminate losses of **$51 to $72 billion** to the worldwide economy through the proper management and protection of machine identities.

Widespread weaponization of machine identities

Machine identity techniques are now incorporated in commodity, off-the-shelf malware with alarming regularity.

TrickBot

"TrickBot has evolved into a universal crimeware solution, offered as-a-service to criminals with modules designed for the needs of specific criminal activities. In 2019, TrickBot added SSH key-grabbing capabilities for both PuTTY (SSH client for Microsoft) and OpenSSH."[4]

Linux Worm

"The Linux worm targets vulnerable Exim mail servers on Unix-link systems to deliver Monero cryptominers. The worm creates a backdoor to the server by adding the attacker's public key to the authorized_keys file and enabling the SSH server if it has been previously disabled."[5]

Skidmap

"This kernel-mode rootkit gains backdoor access to a targeted machine by adding the attacker's public SSH key to the authorized_keys file. Skidmap uses exploits, misconfigurations, or exposure to the internet to gain root or administrative access to the system and drop cryptomining malware."[6]

How can you reduce your machine identity attack surface?

Organizations need a robust machine identity protection solution to:

- **Prevent machine identity theft**
- **Keep up with the explosive growth of machines**
- **Interact safely with new types of machine identities**

To learn how you can start protecting your machine identities visit **venafi.com**

1. IDC. Worldwide Spending on Digital Transformation Will Reach $2.3 Trillion in 2023, More Than Half of All ICT Spending, According to a New IDC Spending Guide. October 28, 2019.
2. Cisco. Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2017–2022. February 18, 2019. Document ID:1486680503328360
3. IDC. IDC FutureScape: Worldwide IT Industry 2019 Predictions. October 2018. Document Number: US44403818.
4. Paloalto. Trickbot Updates Password Grabber Module. November 22, 2019.
5. Cybereason. New pervasive worm exploiting Linux Exim server vulnerability. June 13, 2019.
6. TrendMicro. Skidmap Linux Malware Uses Rootkit Capabilities to Hide Cryptocurrency-Mining Payload. September 16, 2019.

VENAFI®