Nokia Threat Intelligence Report warns of rising cyberattacks on internet-connected devices

Thursday 22 October, 2020

Related Sectors:

Computing & Telecoms ::
Consumer Technology ::

Scan Me:

Report also highlights role of numerous COVID-19-themed cybercriminal campaigns aimed at exploiting user data

Espoo Finland - Cyberattacks on internet-connected devices continue to rise at an alarming rate due to poor security protections and cybercriminals use of automated tools to exploit these vulnerabilities, according to the latest Nokia Threat Intelligence Report.

The report found that Internet-connected, or IoT, devices now make up roughly 33% of infected devices, up from about 16% in 2019. The report's findings are based on data aggregated from monitoring network traffic on more than 150 million devices globally where Nokia's NetGuard Endpoint Security product is deployed.

Adoption of IoT devices, from smart home security monitoring systems to drones and medical devices, is expected to continue growing as consumers and enterprises move to take advantage of the high bandwidth, ultra-low latency, and fundamentally new networking capabilities that 5G mobile networks enable, according to the report.

The rate of success in infecting IoT devices depends on the visibility of the devices to the internet, according to the report. In networks where devices are routinely assigned public facing internet IP addresses, a high infection rate is seen. In networks where carrier-grade Network Address Translation is used, the infection rate is considerably reduced because the vulnerable devices are not visible to network scanning.

The Threat Intelligence Report also reveals there is no let up in cybercriminals using the COVID-19 pandemic to try to steal personal data through a variety of types of malware. One in particular is disguised as a "Coronavirus Map" application – mimicking the legitimate and authoritative Coronavirus Map issued by Johns Hopkins University – to take advantage of the public's demand for accurate information about COVID-19 infections, deaths and transmissions.

But the bogus application is used to plant malware on victims' computers to exploit personal data. "Cybercriminals are playing on people's fears and are seeing this situation as an opportunity to promote their agendas," the report says. The report urges the public to install applications only from trusted app stores, like Google and Apple.

Bhaskar Gorti, Nokia Software President and Chief Digital Officer, said: "The sweeping changes that are taking place in the 5G ecosystem, with even more 5G networks being deployed around the world as we move to 2021, open ample opportunities for malicious actors to take advantage of vulnerabilities in IoT devices. This report reinforces not only the critical need for consumers and enterprises to step up their own cyber protection practices, but for IoT device producers to do the same."

Additional Resources

Webpage: Nokia Threat Intelligence report

Video: Vulnerability in IoT devices

Video: 5G can help secure devices

About Nokia

We create the technology to connect the world. Only Nokia offers a comprehensive portfolio of network equipment, software, services and licensing opportunities across the globe. With our commitment to innovation, driven by the award-winning Nokia Bell Labs, we are a leader in the development and deployment of 5G networks.

Our communications service provider customers support more than 6.4 billion subscriptions with our radio networks, and our enterprise customers have deployed over 1,300 industrial networks worldwide. Adhering to the highest ethical standards, we transform how people live, work and communicate. For our latest updates, please visit us online www.nokia.com and follow us on Twitter @nokia.

Company Contact:

_

Pressat Wire

E. support[@]pressat.co.uk

View Online

Newsroom: Visit our Newsroom for all the latest stories:
https://www.wire.pressat.co.uk