Norton Labs Releases New Consumer Cyber Safety Pulse Report

2021-06-10

Ransomware, Stalkerware, Illicit Coinmining, Gaming Threats and Phishing Scams on the Rise

TEMPE, Ariz.--(BUSINESS WIRE)-- Today, Norton Labs, NortonLifeLock's global research team, launched its first quarterly Consumer Cyber Safety Pulse Report, tapping into the company's breadth of threat telemetry to reveal the top cybersecurity trends from January to March 2021. Phishing campaigns remained the number one threat to consumer Cyber Safety, with top scams relating to the pandemic, including vaccine-oriented, financial relief, and tech support scams[1].

(Graphic: Business Wire)

"Our renowned Norton Labs group is at the forefront of identifying and analyzing the latest trends in cybercrime, and it's clear through their analysis that cybercriminals continue to find new ways to capitalize off of the pandemic," says Darren Shou, head of technology, NortonLifeLock. "Over the next three months, we can expect scammers to tap into the gradual shift to a post-COVID state as people start to return to work, travel and engage in social activities."

Norton blocks more than 900 million threats on average every 100 days. Between January 2021 and March 2021, 49.6 million phishing attempts, 46.3 million file-based malware, 686,000 mobile-malware files and 536,137 ransomware detections were reported. During this time, the majority of scams were designed to trick consumers into sharing their personal and financial information in an attempt to steal their money.

Additional insights from the Consumer Cyber Safety Pulse Report include:

- **Popularity of cryptocurrency is driving spikes in illicit coinmining and ransomware:** Coinmining has come roaring back with the price of Bitcoin quadrupling over the past year. Cybercriminals are taking advantage of the price trend and increasingly spreading coinminer malware that exploits consumers' computer resources (i.e., processor, graphics card, memory and network bandwidth) for illicit mining activities – victims could see a spike in their electric bills as a result.

  Similarly, now that consumers have easy access to cryptocurrencies through services like Coinbase, Robinhood and PayPal, there has been a parallel rise in ransomware campaigns requiring payment in cryptocurrency, with a 35% increase from late 2020 to early 2021.
- **Cybercriminals continue targeting gamers:** In addition to phishing campaigns, "Trojanized" crack campaigns are an increasing threat targeting the gaming community. These cracks are being distributed from sites that show up very early in Google searches and trick gamers into manually disabling antivirus protection while infecting their system with a variety of highly malicious software.
- **Stalkerware on the rise:** Instances of stalkerware, malware designed to secretly monitor victims'

activities on their devices, increased by 20% from November 2020 to January 2021. Norton Labs also detected a surge in emails purporting to sell stalkerware.

For more information and Cyber Safety guidance, visit the Norton Internet Security Center.

About NortonLifeLock Inc.

NortonLifeLock Inc. (NASDAQ: NLOK) is a global leader in consumer Cyber Safety, protecting and empowering people to live their digital lives safely. We are the consumer's trusted ally in an increasingly complex and connected world. Learn more about how we're transforming Cyber Safety at www.NortonLifeLock.com.

---

[1] No one can prevent all cybercrime or identity theft.

Jenna Torluemke
NortonLifeLock Inc.
(650) 527-6015
Jenna.Torluemke@nortonlifelock.com

Heaven Lampshire
Edelman for NortonLifeLock Inc.
(541) 852-7885
Heaven.Lampshire@edelman.com

Source: NortonLifeLock Inc.