IDENTITY THEFT

TRENDS IN 2021

In the next year, the Identity Theft Resource Center (ITRC) predicts identity theft protection services will primarily focus on data breaches, data abuse and data privacy. ITRC also predicts that consumers will become more knowledgeable about how data breaches work and expect companies to provide more information about the specific types of data breached and, in general, will demand more transparency in data breach reports.

Cyber attacks are more ambitious
According to a 2019 Internet Security Threat Report by Symantec, cybercriminals are diversifying their targets and using stealthier methods to commit identity theft and fraud. Cybercrime groups like Mealybug, Gallmaker and Necurs are opting for off-the-shelf tools and operating system features such as PowerShell to attack targets.

- Supply chain attacks are up 78%
- Malicious PowerShell scripts have increased by 1,000%
- Microsoft Office files make up 48% of malicious email attachments

Internet of Things threats on the rise
Cybercriminals attack Internet of Things (IoT) devices an average of 5,233 times per month. Routers and connected cameras were the main targets of IoT attacks in 2018, accounting for about 90% of activity. IoT attacks involving connected cameras increased by about 12% in the last year as well. According to Symantec, cybercriminals most often access IoT devices by using the passwords: 123456, [BLANK], system, sh, shell, admin, 1234, password, enable and 12345.

Formjacking is up 117%
Formjacking is when cyber criminals inject malicious Java Script code to hack a website and take over the functionality of the site's form page to collect sensitive user information. More than 57,800 unique websites were compromised by formjacking last year, and cybercriminals continue to take in millions each month by hijacking credit card data from online payment forms.

Ransomware activity is down 20%
Ransomware attacks decreased last year for the first time since 2013 — identity theft experts suspect this is because ransomware attacks target Windows-based applications and more people are storing and sharing data using the cloud. Ransomware threats remain a risk for businesses, as enterprise ransomware has increased by 12%.

New account fraud is up 13%
Last year, new account fraud accounted for $3.4 billion in losses, up from $3 billion the year before, according to Javelin Strategy. The most common targets for new account fraud are mortgages, student loans, car loans and credit cards.

Account takeovers are up 79%
The number of account takeovers also increased, rising from 380,000 in 2017 to 679,000 in 2018. Both individuals and enterprises are at risk for account takeovers.

Fortaris Capital Advisors specializes in addressing these threats with a comprehensive Threat and Risk Assessment process. Call today to arrange a consultation.

FORTARIS CAPITAL ADVISORS

Fortaris Capital Advisors delivers over 50 years of leadership expertise with a proven track record of implementing innovative solutions to improve profitability, mitigate risks and maximize stakeholder value.

The Fortaris team is expert in their field providing corporate security, fraud investigation, cyber-security and financial management solutions for companies of all sizes, across numerous industries. From start-ups to mature companies facing restructuring, the team brings the know-how and tools needed to safeguard and protect against the menacing threats to business continuity in today's evolving global marketplace.

Fortaris Capital Advisors is a fully licensed and insured advisory and private investigation firm.

To learn more about our services, visit us online. To arrange a consultation, contact our team of professionals. You will receive a response within 24 hours.

KEVIN M. CRONIN
PRINCIPAL
248.410.3839
kevin.cronin@fortariscapital.com
www.fortariscapital.com