The Financial Industry's Path of Most Resistance

Cybersecurity Series

By Tony Lutz, Chief Technology Officer Finance, Verizon Business

Last year, simple errors were among the top few causes of most data breaches in the financial services industry. System intrusion, miscellaneous errors, and social engineering were the most common culprits. This year, system intrusion has overtaken miscellaneous errors and basic web application attacks as the primary threat in the industry, suggesting a shift toward more complex attacks – a trend that has coincided with the rise of social engineering. The financial services industry stands to lose much from cyberattacks, both financially and reputationally. Financial organizations must understand the evolving nature of the threat to effectively mitigate the risk.

The path of most resistance

For years, we at Verizon Business have sought to debunk an enduring myth about a lot of threat actors: that they are criminal masterminds who avail themselves of the most cutting-edge technologies. In truth, a large number of malicious actors seek the easiest paydays, but when those paydays become more elusive, they find other means. According to the 2023 Data Breach Investigations Report (DBIR), the system intrusion pattern, responsible for most complex attacks, was the third-most common pattern. In contrast, the 2024 DBIR found it to be the most common. Meanwhile, basic web application attacks, which occupied the number one slot in the 2023 DBIR, have fallen out of the top three patterns.

Social engineering, which can also include more sophisticated attacks, is among the top three patterns. Pretexting, which refers to threat actors masquerading as trusted individuals and institutions so as to compel network users to divulge sensitive information, can be especially sophisticated. Additionally, it's central to business email compromise (BEC) attacks, which can be quite costly to an organization.

verizon business

Will AI become a factor?
Another element worth keeping an eye on is the role AI may play in pretexting (and social engineering in general) in the coming years. Though we haven't seen evidence to suggest AI has played an appreciable role in pretexting, it's hard to ignore its many potential applications for pretexting. The latest iteration of generative AI boasts sophisticated natural language processing capabilities, which not only could mimic the speech patterns of individuals, but it could also enable threat actors to scale credible pretexting attacks across different countries and languages. AI's ability to replicate voice is also compelling, which could in theory supercharge vishing attacks.

That's not to say that AI will become a go-to hacking tool in the upcoming years, but rather to point out that tactics change depending on opportunities, pressures, and needs – just like any marketplace. Pretexting and vishing have been effective without the aid of AI, but if they become less effective, threat actors may explore other options. In retail this year, for instance, phishing was down but pretexting was up, which may be an early indicator that some of the easier routes are not working as well for hackers.

None of this is a guarantee. Basic web applications could rise again next year. The broader point is that it's important to track patterns so as to tailor cybersecurity programs to the most persistent threats and to allocate resources accordingly.

Transparency in the age of interconnectedness
I'd be remiss if I neglected to note that 8% of the cases in this year's DBIR's incident dataset for this sector were part of last year's MOVEit breach. Not only does that demonstrate how far-reaching supply chain breaches can be, but it also underlines the interconnectedness of today's data ecosystem. Zero-day exploits aren't the only threats that reveal the weakness of this emergent dynamic. Partners, vendors and other third parties can also compromise organizations. One's cybersecurity is only as strong as its weakest link, after all.

The financial industry faces the additional burden of regulatory compliance due to the SEC's recent cybersecurity disclosure requirement. Failure to comply with these regulations while experiencing a data breach results in penalties, fines, and reputational damage. These consequences can be particularly severe for publicly traded companies, as their reputation is crucial for investor confidence and market success.

The cybersecurity challenges of the financial industry are complex, given the regulatory layer they must contend with, but the silver lining is that the Wall Street CISO now has a more prominent seat at the table, which bodes well for the security of the financial sector.