IBM Security

Financial services: still the #1 target for cybercriminals

The scale and sophistication of attacks are on the rise. Attackers are stealing directly from customer bank accounts and intercepting online transactions. Organized cybercrime syndicates are targeting entire financial networks to maximize operational disruption and monetary gain. The malware behind these operations continues to deceive and multiply as it becomes easier to deploy and harder to detect.

MOST FREQUENTLY TARGETED INDUSTRY TWO YEARS IN A ROW

2017

27% of all security incidents[1]

17% of all attacks[1]

148M records breached[2]

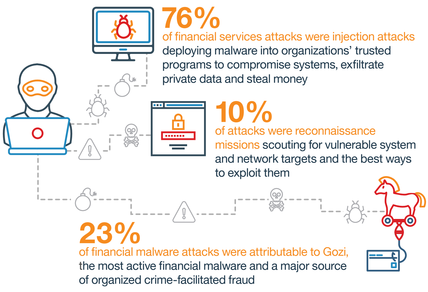
Security incident: A security event that has been reviewed by IBM and deemed worthy of deeper investigation

Attack: Malicious activity attempting to collect, disrupt, deny, degrade or destroy information or system resources

[1] IBM X-Force® Threat Intelligence Index 2018. [2] IBM X-Force Exchange: X-Force 2017 Data Breach Review.

INJECTION ATTACKS DOMINATED

Attackers are systematically exploiting unpatched vulnerabilities, penetrating bank infrastructures, ATMs, capital management funds and cryptocurrency exchanges and launching destructive distributed denial of services (DDoS) attacks to hurt and extort organizations.



76%
of financial services attacks were injection attacks deploying malware into organizations' trusted programs to compromise systems, exfiltrate private data and steal money

10%
of attacks were reconnaissance missions scouting for vulnerable system and network targets and the best ways to exploit them

23%
of financial malware attacks were attributable to Gozi, the most active financial malware and a major source of organized crime-facilitated fraud

IBM X-Force Threat Intelligence Index 2018.

THE COSTS ARE HIGH AND GETTING HIGHER

While the average cost of a lost or stolen record fell 2.9 percent across industries, it increased in financial services.

Average global cost per lost or stolen record for financial services $245

11%
higher than the cost per lost or stolen record the prior year ($221)

74%
higher than the cross-industry average ($141)

2nd
most significant increase in cost over four years compared to other industries ($23)

A financial services breach can result in customer loss that is nearly 6% higher than normal

*2017 Cost of Data Breach Study," Ponemon Institute, Sponsored by IBM, June 2017.

5 STEPS YOU CAN TAKE TO PROTECT YOUR CUSTOMERS AND YOUR COMPANY

1 Leverage the power of cognitive technologies

Improve your security analysts' response to threats using expert systems—artificial intelligence and machine learning technologies—to make sense of structured and unstructured data

2 Deploy ample data security and privacy measures

Satisfy mounting governance, risk and compliance requirements by implementing better data protection, access controls and monitoring

3 Get ahead of threats by preparing in advance

Achieve better control over security incidents and breaches by incorporating security intelligence, incident response and remediation into a strategic playbook

4 Go on the vulnerability offensive

Identify and exploit vulnerabilities across all target types (applications, network, hardware, and human) before your adversaries do through robust scanning and testing services

5 Practice good security fundamentals

Back up data, educate users with cybersecurity awareness programs, and stay on top of system and software updates and patches

Larger, more sophisticated attacks are on the horizon. Your organization doesn't have to fall victim to them. IBM Security delivers the technologies and expertise to defend against evolving threats with real-time security intelligence, continuous monitoring, and automated risk and compliance management.

FIND OUT HOW IBM SECURITY CAN HELP

LEARN MORE

IBM

08015708-USEN-00