
2019 Data Breach Investigations Report

Availability

Confidentiality

Integrity

Unparalleled reach into breach insights.

For security practitioners. Written by security practitioners.

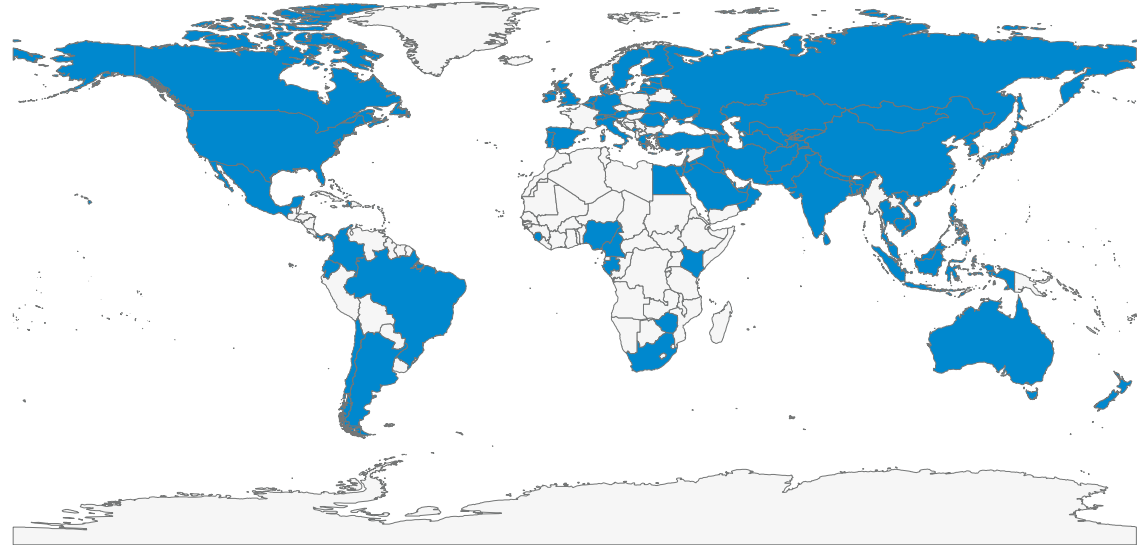
12 years

86 countries

73 contributors

41,686 security incidents

2,013 data breaches



Key Insights

C-level executives increasingly and proactively targeted by social breaches

Senior executives are 12x more likely to be the target of social incidents, and 9x more likely to be the target of social breaches than in previous years – and financial motivation remains the key drive.

Financially-motivated social engineering attacks (12%) are a key topic in this year's report, highlighting the critical need to ensure ALL levels of employees are made aware of the potential impact of cybercrime

Attacks on Human Resource personnel have decreased from last year.

Findings saw 6x fewer of those professionals being impacted this year compared to last, correlating with the W-2 scams almost disappearing from the DBIR dataset.

Shift in payment card compromises

The number of payment card web application compromises is close to exceeding the number of physical terminal compromises in payment card related breaches.

Key Insights – FBI IC3 Breach Cost Analysis

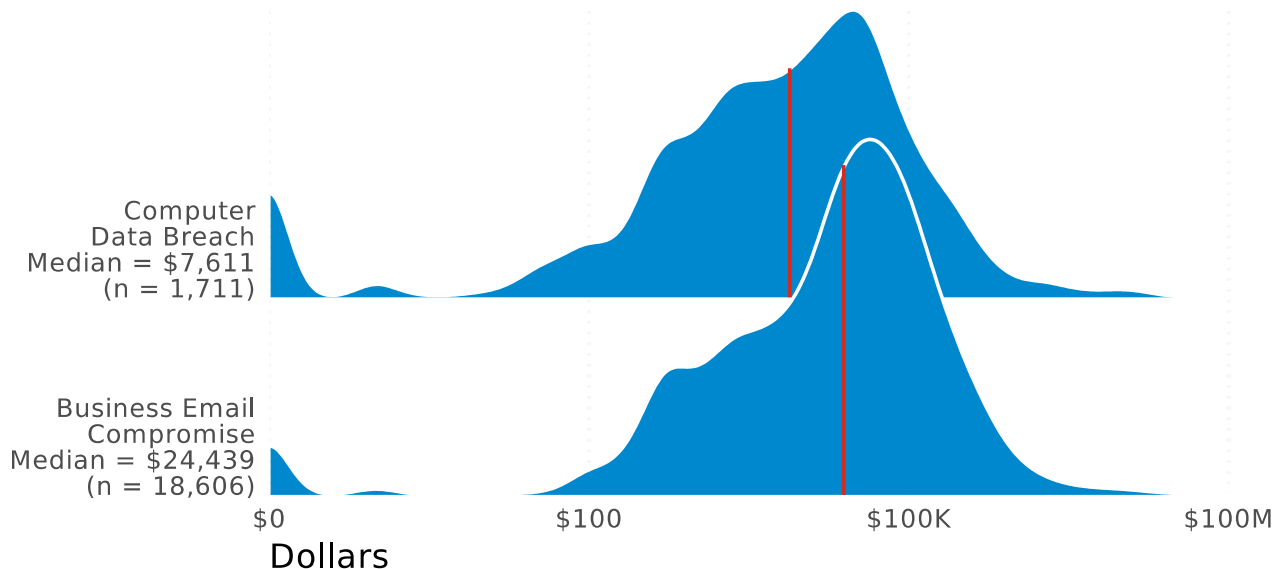
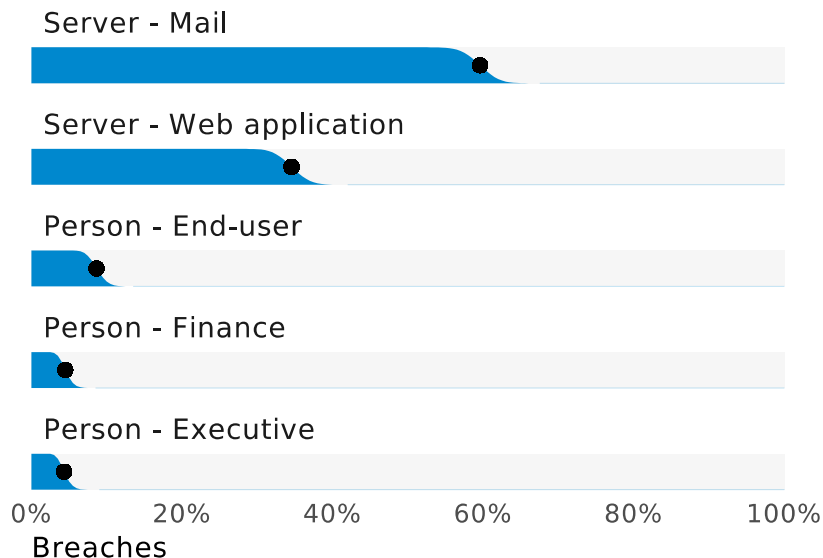
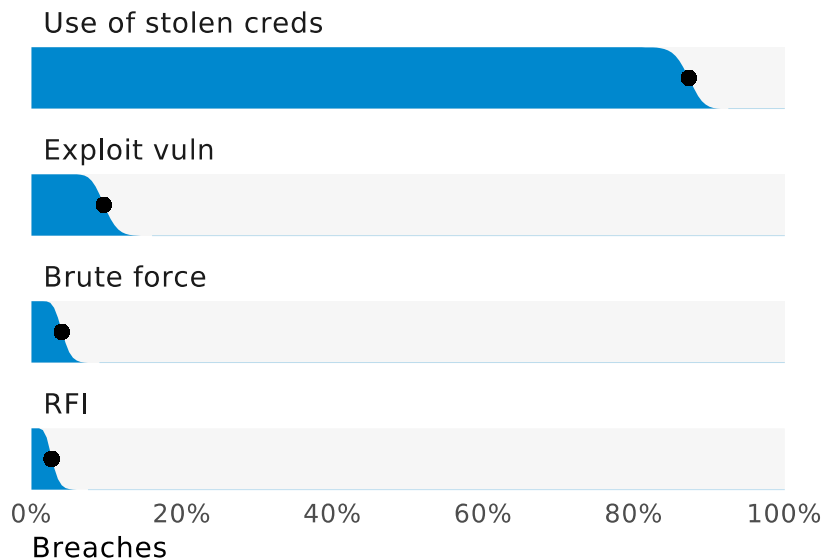


Figure 37. Amount stolen by breach type

Key Insights – Cloud-based E-mail Compromises



Top assets in webapp hacking vector breaches, n=579



Top hacking varieties in webapp hacking vector breaches, n=448

Key findings – Cloud Misconfigurations

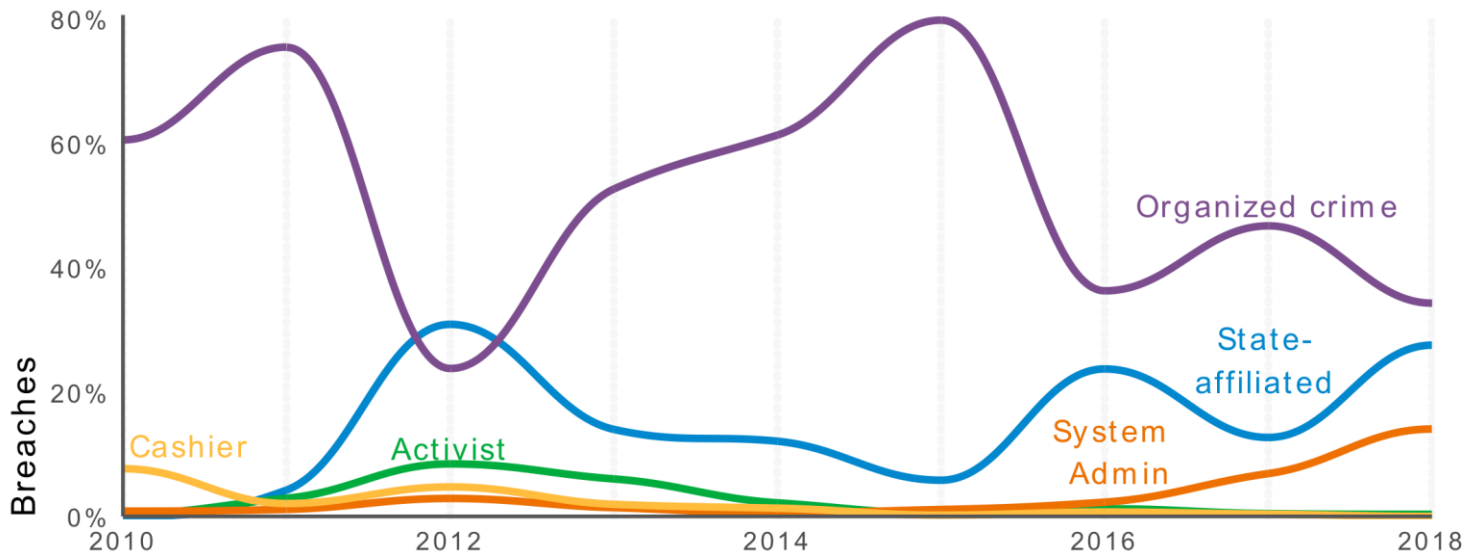


Figure 8. Select threat actors in breaches over time

Key Findings – Threat Actors

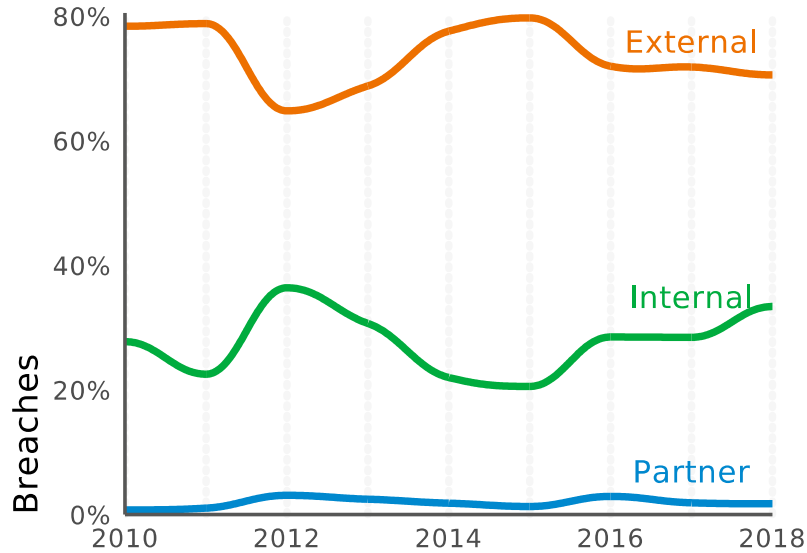


Figure 6. Threat actors in breaches over time

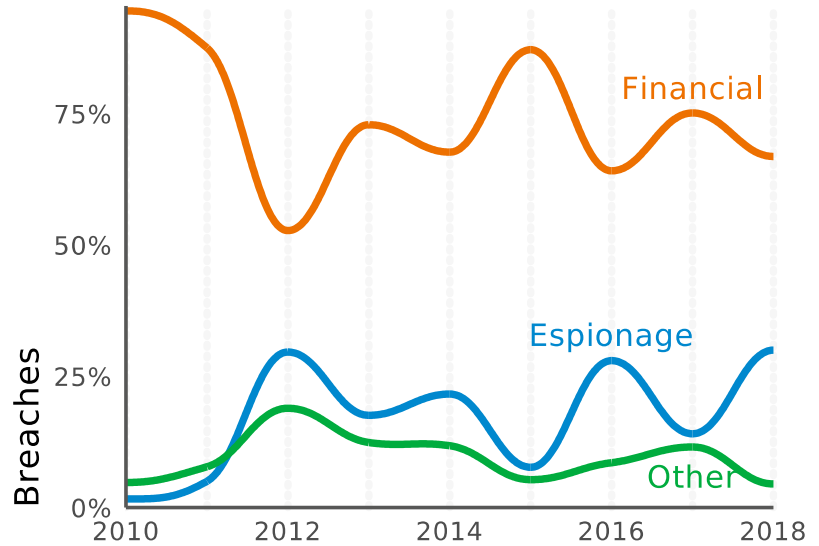


Figure 7. Threat actor motives in breaches over time

Unbroken Chains - Shorter paths are more common

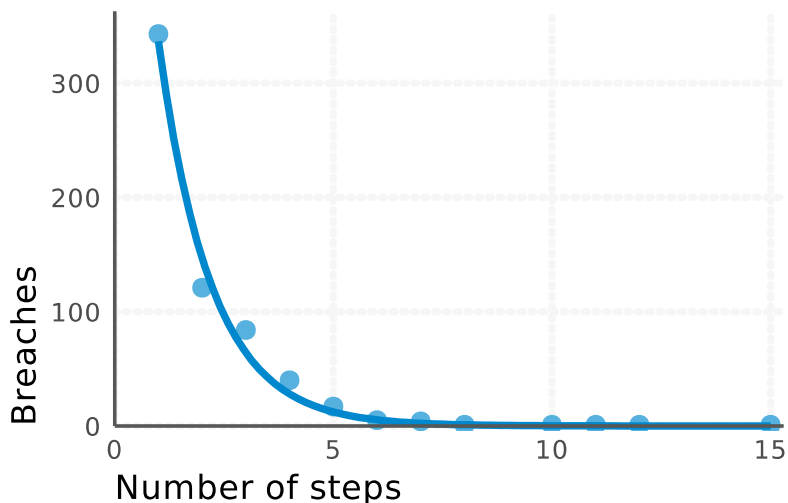


Figure 29. Number of steps per incident (n=941)
Short attack paths are much more common than long attack paths.

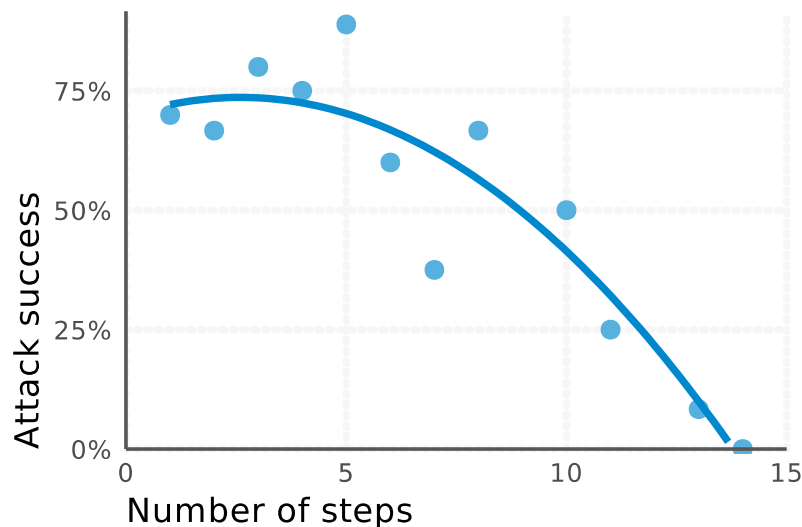
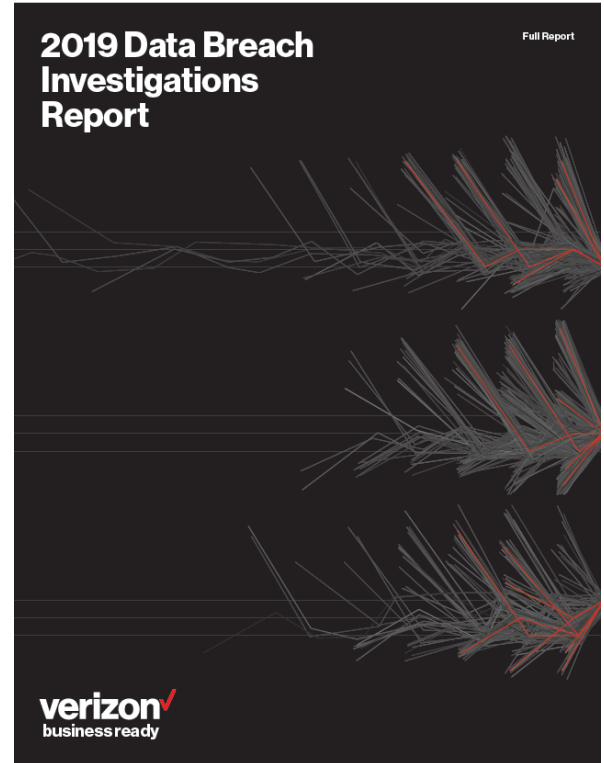


Figure 34. Attack success by chain length in simulated incidents (n=87)

Wrapping up – Main Takeaway

“The more things change, the more they stay the same”.

- While we have observed a definite shift in attacker behavior towards cloud-based services for email and online payment card processing systems, this does not indicate that there are necessarily any inherent weaknesses associated with those environments.
- Instead, we believe this to simply be a result of the attacker changing tactics and targets to meet the corresponding change in the locations of valuable corporate assets.
- As the victim organizations increasingly migrate to cloud based solutions, the attackers must alter their actions in order to access and monetize those assets.
- The evolving job of the CISO/CSO is to understand how this large-scale digital relocation changes the landscape, and how they can make known risk vectors more or less likely.



Questions?

- Twitter: @VZDBIR
- E-mail: dbir@verizon.com

