WELCOME TO THE GEMINI IBD® INFOGRAPHICS NEWSLETTER

[VOLUME 18] 12-10-2022

DATA BREACHES FOR 2022

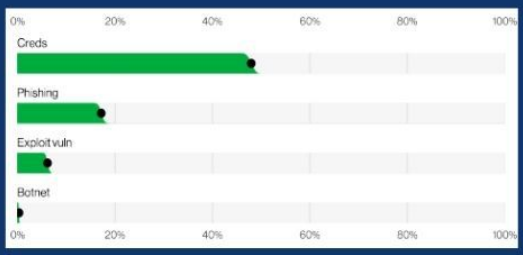
Well, here we are now close to the end of the year of 2022. True, lots of things have happened all over the world, especially on the geopolitical front. There was even fear of nuclear war, the first talk about this to come into existence since the Cold War which, was decades ago. There are also have been some unique trends in the Cyber Landscape as well, many feared an onslaught of attacks from Russia as it invaded the Ukraine. Insurance companies have greatly ratcheted up their requirements before and applicating will be awarded a Cyber Policy, and even self attestation will not work.

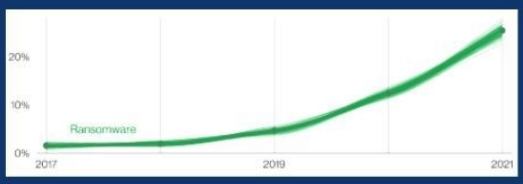
Thus, many SMB owners now have to get an outside party to confirm that their lines of defenses are up and ready, and present that to the insurance carrier. We've probably seen more attacks on our Critical Infrastructure more than ever before, but they have been isolated incidents. But the trends are now for the Cyberattacker to use OSINT related tools to hunt down their victims, especially using Social Media as the way to do this. There is also fear that Social Engineering and other lower tech kinds of Cyberattacks will now start to evolve.

But whatever the trends may be for 2023, there is one common denominator that will still dominate the news headlines: Data breaches. In this last newsletter of the year, we look at some of them that transpired in 2022, and will likely roll over into next year.

SUMMARY OF KEY FINDINGS FOR 2022

There are four key paths leading to your estate: Credentials, Phishing, Exploiting vulnerabilities and Botnets. These four pervade all areas of the DBIR, and no organization is safe without a plan to handle them all. This year Ransomware has continued its upward trend with an almost 13% increase–a rise as big as the last five years combined (for a total of 25% this year). Supply chain was responsible for 62% of System Intrusion incidents this year. Error continues to be a dominant trend and is responsible for 13% of breaches. The human element continues to drive breaches. This year 82% of breaches involved the human element.





TRENDS IN DATA BREACHES FOR 2022

Research indicate that data compromises are considerably more likely to result from external attacks than from any other source. Nearly three out of four cases yielded evidence pointing outside the victim organization. Internal sources accounted for the fewest number of incidents (18 percent), trailing those of external origin by a ratio of four to one. The relative infrequency of data breaches attributed to insiders may be surprising to some. It is widely believed and commonly reported that insider incidents outnumber those caused by other sources. While certainly true for the broad range of security incidents, research showed otherwise for incidents resulting in data compromise.

THE IMPACTS OF RANSOMWARE FOR 2022

The system intrusion pattern consists of more complex breaches and attacks that leverage a combination of several different actions such as Social, Malware and Hacking and is where we find Supply Chain breaches and Ransomware, both of which increased dramatically this year. This pattern also continues to see the Use of stolen credentials and malware, such as Ransomware, as the top concerns.

Frequency	7,013 incidents, 1,999 with confirmed data disclosure
Threat Actors	External (98%), Internal (2%) (breaches)
Actor Motives	Financial (93%), Espionage (6%) (breaches)
Data Compromised	Credentials (42%), Personal (37%), Other (35%), Internal (16%) (breaches)

It is highly expected that in 2023, Ransomware attacks will start to pick up in stealthiness and covertness. For example, there are many Ransomware gangs that have stayed silent this year, but will make a very aggressive move in 2023. We will probably see many more Business Email Compromise attacks (BEC) because that relies more on Social Engineering. Cyberattackers will move from targeting digital assets to now Physical Assets. So make sure that your lines of defenses are beefed up for that.

Finally, the Zero Trust Framework will pick up more steam as companies try to mitigate their risk in becoming an actual Cyberattack victim.