Protecting Yourself and Your Business Today from New Threats Tomorrow

The cybernetic threat landscape is constantly changing, and smart businessmen and women know to stay ahead of the curve. This article discusses changes in the threat landscape from 2018 to 2019, taken from the IBM X-Force Threat Intelligence Index, providing valuable insights into attacker methods and motivations as well as detailing the steps you should take to make sure you won't become the victim of a cyberattack. If you would prefer to view the full report in detail for yourself, please follow the link below, if not, continue reading our interpretation of the data.

https://www.ibm.com/account/reg/us-en/signup?formid=urx-42703

First, let's take a look at the most common initial infection vectors. In 2019, these vectors rated very close together. Phishing made up 31%, Scan and Exploit 30%, and Stolen Credentials 29%.

In 2019 phishing was the most popular method but attackers increasingly scanned targets to exploit their weaknesses, showing a significant increase from 8% to 30% over the past year. The use of stolen credentials where threat actors use previously obtained credentials to access targets came in at a close third at 29 %. These credentials are often stolen from a third party site or obtained using a phishing attempt against the target. Threat actors can use stolen credentials to blend in with legitimate traffic, making detection much more challenging. Brute force attacks decreased dramatically to fourth place with 6 percent of all cases, followed by BYOD at 2 percent as the initial access point into targets.

Concerning frequency of attacks, a significant increase in threat actor activity was observed in the summer of 2019, with the number of events going beyond totals for all of 2019 up to that point. While we do not know the reason for this sudden increase in activity, the summer months appear to be more active concerning spam as well, with peak spam volume being recorded in August of 2019. It's possible that threat actors were simply careless and more easily spotted, or that a change in threat actor tactics or tools stimulated this rise in activity. Short term areas of high activity are less likely the result of the appearance of new threat actors, as such new entries would be expected to create a sustained increase in activity rather than a temporary one.

Global spam trends in general show a reliance on old, tried-and-true methods as opposed to new ones. IBM's analysis of global spam activity shows that spam email continues to focus on a limited area of vulnerability, with focus on only two CVEs: 2017-0199 and 2017-11882. Together, these two vulnerabilities made up almost 90% of the vulnerabilities used by threat actors for spam campaigns. Both these CVEs affect Microsoft Word and do not require user interaction beyond simply opening a tainted document.

While these two vulnerabilities appear in large amounts of spam email, there is no indication as to how successful they might be in actually exploiting users. However, spam is often a numbers game and with enough volume, even a small success rate is enough to

generate value for threat actors. Because many users and even organizations can lag behind on fixing certain issues, it is still possible to see devices compromised by such older bugs.

As one might expect, threat actors' priorities have shifted over the past year. In today's threat landscape, the specificity of some types of attacks according to threat actor motivations means cybersecurity risk management can look very different from one sector to another. Although Financial Services remained in the lead as the most targeted sector in 2019, growth in other sectors showed threat actors' shifting attention and priorities, with Retail, Media, Education, and Government all advancing on the global chart of most targeted sectors. While there were no surprises concerning financial services, the retail industry has been gathering increased interest from attackers. The same is true for media and entertainment companies, education, and government agencies.

Although the threat landscape is constantly changing and evolving, there are a few tools you can use to protect yourself from threats, new and old alike. DMARC analysis is a new and growing email analysis tool that is sure to make a big splash soon. It effectively monitors your sending domains, allowing you to see which sources are sending on behalf of your domain and make sure that all your legitimate sending sources comply with SPF, DKIM and DMARC, ensuring email deliverability. With DMARC analysis it is also possible to monitor the health of your email sending system over time and detect any email spoofing or phishing attacks.

GlockApps also offers email tests to ensure your emails are spam free and will make it to the inbox. These tests identify risky content that could otherwise lead to your email being flagged as spam and not getting delivered. We also offer Inbox Rate Tracking, which tracks your inbox, spam, and missed percentages to give you the most accurate and comprehensive information about your inbox placement by campaign.

In today's changing threat landscape you cannot afford to be unprotected. GlockApps provides you with the cutting-edge tools needed to protect yourself from dangers online and ensure the success of your email and website. We hope this article has shed some light on new and emerging cyber threats and has provided you with the information necessary to protect yourself. If you are interested in further details, a link to the full report from IBM is located below for your convenience.

https://www.ibm.com/account/reg/us-en/signup?formid=urx-42703