The State of Phishing

In 2022, cybercriminals are moving with speed and at scale. Mobile phishing and credential harvesting are exploding, causing breaches in places once thought impenetrable. With billions of dollars, company reputations, and personally identifiable information at stake, advanced phishing protection is vital for all businesses.

EXECUTIVE SUMMARY

Since we last published our State of Phishing Report in 2021, some trends remain the same and much has changed. What is consistent is that phishing continues to explode. Hybrid work and the use of personal mobile devices for work continue to be a trend, and the bad actors are taking full advantage of the fact that many security technology vendors cannot keep up. What has changed is important.

Imagine the familiar metaphor of Whac-A-Mole when thinking about cybersecurity professionals trying to stop one phishing attack, only to see another new attack pop up someplace else. That metaphor no longer describes the state of phishing. Today the appropriate metaphor is The Matrix fight scene where Neo fights 195 Smiths at once, and the potential for Smith to morph and multiply is endless.

However, it's not all doom and gloom. This report demonstrates how phishing has changed through the lens of cybersecurity technology. We can only present the data in this report because technology is available to detect these trends and stop more threats. For example, at the end of 2021, we detected 50,000 malicious URLs daily, a 68% increase from the start of the year. Less than 12 months later, we detected 80,000 malicious URLs daily, which is another 61% increase. This equates to 255M phishing attacks detected in 2022. Certainly, there is an increase in phishing, and as cybersecurity tools improve, the industry is also detecting and stopping more attacks.

Finally, this report will dive into some of the most pervasive threats, including the shift to multi-channel phishing, sophisticated credential harvesting on email, and the massive increase in threats emanating from trusted services. With an 80% increase in threats from trusted services in 2022, we started to track these threats in a unique database in 2022.

IN THIS REPORT

- What big trends from 2021 continued in 2022, and what this likely means for the future
- Mobile, mobile, mobile — And other personal communication channel threats
- Email trends with Microsoft and ICES
- Threats menacing trusted services and the top 10 services hackers use for attacks
- Summary of key findings
- How an integrated, multi-channel security approach is needed

Report data and methodology: The report data is taken from a sample of threats detected by SlashNext security products. SlashNext analyzed over a billion link-based, malicious attachments and natural language threats scanned in email, mobile and browser channels over six months in 2022. The organizations in our sample ranged in size from 500 to 100,000 users. The organizations spanned a variety of industries in North America.

The threat data in the report is gathered using SlashNext's Two-Phase AI Detection, which uses virtual browsers, machine learning, and LiveScan™. This approach detects live and emerging zero-hour threats. Our cloud-based AI detection is preemptive with proactive threat hunting to detect phishing, scams, malware, and exploits, revealing approximately 700,000 attacks a day. Secondarily content is analyzed in real-time with LiveScan™ to reveal zero-hour threats automatically.

BIG TRENDS

People are the most vulnerable part of an organization when it comes to phishing, scams, and fraud. They are also the most unprotected across all communication channels. For hackers, phishing is the most effective and far-ranging tool to perpetrate cybersecurity breaches, including lucrative ransomware and data theft.

In 2021 we highlighted several high-profile breaches that started with phishing, and that trend continues. From pre-pandemic 2019 to post-pandemic 2022, phishing has increased consistently, with a 61% jump in malicious URLs from 2021 *(Exhibit 1)*. The jump in malicious URLs equates to 255M phishing attacks detected in 2022. 76% of the attacks found in 2022 were credential harvesting, which is still the number one cause of breaches, as demonstrated in the high-profile breaches in 2021 and again in 2022 with Twilio, Cisco, and Uber, all starting with credential theft.

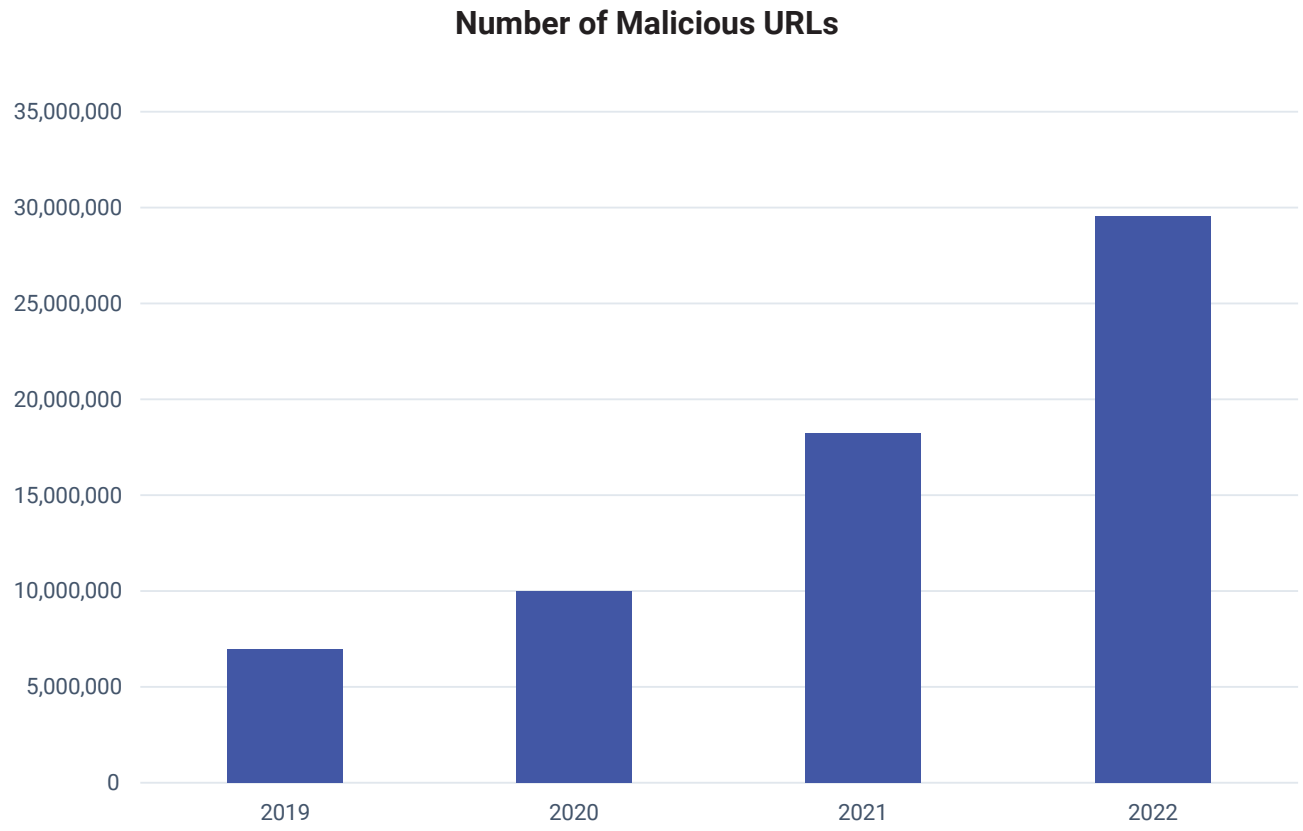

Exhibit 1: Malicious URLs from 2021 to 2022 has increased by 61%, equating to 255M phishing attacks detected in 2022.