Current Malware and Security Breaches and How to Defend Against Them

Successful military leaders know their enemies and the threats they present. This allows them to mount the right defense. Wise business leaders use the same tactic. Understanding current malware and security breaches that dominate the threat environment informs security strategy.

Cyber attacks in the news in the first half of 2022 show ransomware on the rise again. Additionally, hacker gangs have abused weak cyber security postures, exploiting insider threats and social engineering to gain network access. In many cases, basic security practices, including strong security awareness training programs, would have thwarted the attacks.

Ransomware on the Rise

After a decline in ransomware in 2021, ransomware attacks have begun to rise again. In fact, the first quarter of 2022 saw twice as many ransomware attacks as reported in the entire previous year. While high profile attacks on Colonial Pipeline, Apple and JBS gathered attention in 2021, hackers seem to be turning their focus to small and midsize businesses (SMBs).

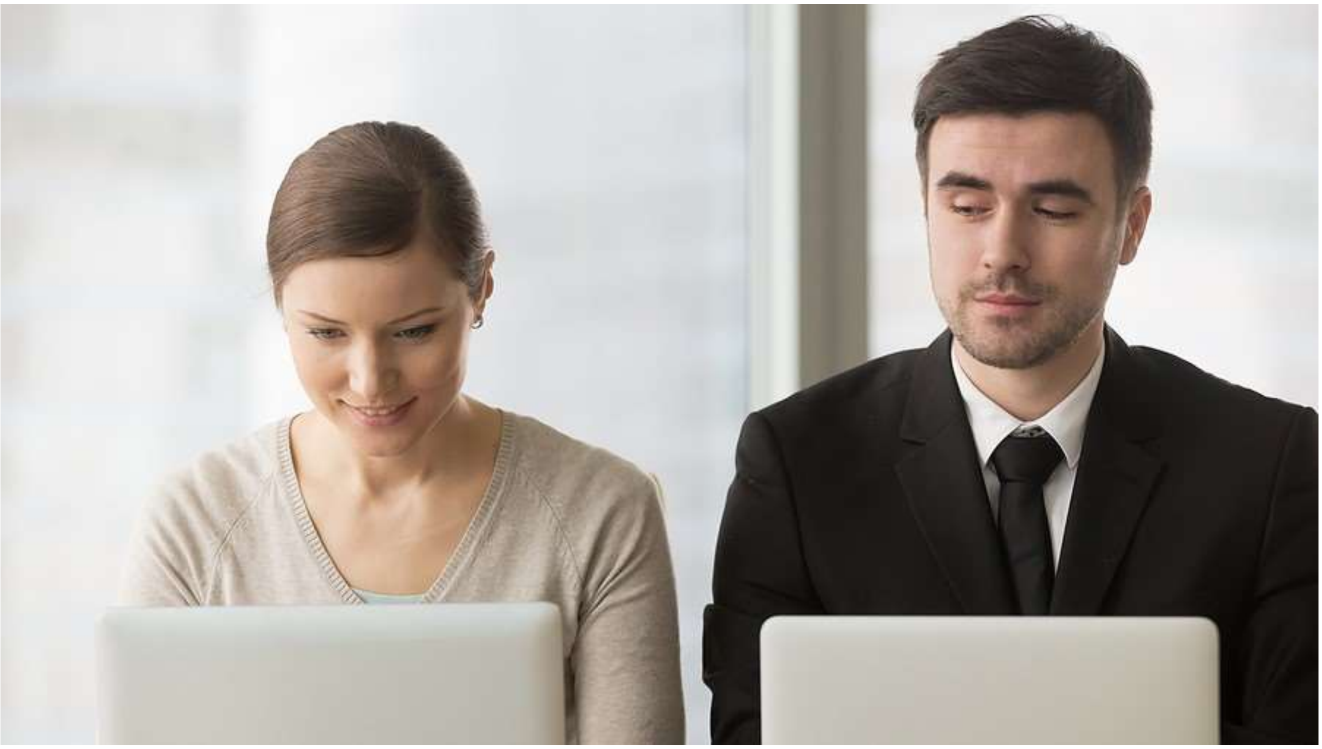
Experts suspect a couple of reasons for this shift. In the first place, SMBs tend to invest significantly less on cyber security than large enterprises, making them easier targets. Also, attacking smaller organizations allows hackers to fly under the radar more effectively.

RansomHouse Gang Takes Advantage of Bad Passwords

Recently, the RansomHouse gang announced that it had stolen 450 GB of sensitive data from semiconductor giant AMD. RansomHouse seems to have appeared on the scene near the end of 2021, previously hijacking targets in Africa and Canada. In this instance, the gang mocks poor passwords at AMD that effectively left a door wide open for bad actors.

"Even technology giants like AMD use simple passwords to protect their networks," wrote RansomHouse. The post revealed that AMD employees used well known passwords such as "123456" and "password."

Due to the amount of valuable data RansomHouse claims to have acquired, they have not demanded a ransom from AMD. Instead, they have determined that selling the data on the black market will prove more lucrative.



Lapsus$ Hacker Group Exploits Insider Threats

Another hacker group, Lapsus$, has also carried out significant attacks this spring. Using social engineering, the group exploits insider threats to gain entrance to its victim organizations. In the case of Microsoft, for instance, they took over a single account, then compromised several key projects. Fortunately, customer data remained safe.

Authentication company Okta also fell prey to the group. In March, Lapsus$ compromised a vendor that provided support for Okta. By accessing the account of a support engineer, hackers exploited a connection to Okta's environment.

Okta maintains that its zero trust procedures prevented Lapsus$ from fully taking over the compromised account. However, the company has had to work hard to reestablish trust with its customers, which include JetBlue, T-Mobile and Albertsons.

Top Malware Threats Employ Social Engineering

Social engineering features prominently in lists of top malware threats published by security experts this spring. For instance, the Shlayer virus continues to plague organizations by using malvertisements (malicious advertisements) to spread malware. Clicking the fake ads, often for Adobe Flash Player updates, leads victims to unwittingly install malicious code.

Similarly, hackers send emails regarding an "urgent Windows OS update" that users must install. The supposed update actually installs ransomware instead. Other attacks reference current news, such as ongoing COVID concerns, to tempt readers to click a link.

Thwart Malware and Security Breaches with Essential Security Practices

By implementing essential security practices, organizations can guard against most of these threats. Specifically, critical practices include updating password policies and deploying multi-factor authentication (MFA), as well as strengthening email filters. Additionally, organizations guard against social engineering by increasing security awareness among all employees.

eMazzanti delivers the security tools necessary, from email defense to MFA, employee training, 24/7 network monitoring, and more.