Online Attacks Against Small Business *on the Rise*

carmichael consulting solutions

Small business owners often believe their size protects them from nefarious online actors' hacks, but nothing could be further from the truth. In fact, online bad guys who launch Trojans disguised as Microsoft Office files, hacks, ransomware demands and phishing emails, account for 58% of small business breaches. Despite that, 54% of small business owners continue to think their enterprises are too small to attract the attention of online scammers. And if feels like these attacks are proliferating, you are right. Last year, breaches of small business networks were up 424%.

WHY MONITORING FOR EXPOSED CREDENTIALS IS IMPORTANT

PHISHING
- Send e-mails disguised as legitimate messages
- Trick users into disclosing credentials
- Deliver malware that captures credentials

WATERING HOLE
- Target a popular site: social media, corporate intranet
- Inject malware into the code of the legitimate website
- Deliver malware to visitors that captures credentials

MALVERTISING
- Inject malware into legitimate online advertising networks
- Deliver malware to visitors that captures credentials

WEB ATTACK
- Scan Internet-facing company assets for vulnerabilities
- Exploit discovered vulnerabilities to establish a foothold
- Move laterally through the network to discover credentials

Passwords are a twentieth-century solution to a modern-day problem. Unfortunately, user names and passwords are still the most common method for logging onto services including corporate networks, social media sites, e-commerce sites and others.

39%
Percentage of adults in the U.S. using the same or very similar passwords for multiple online services

28,500
Average number of breached data records, including credentials, per U.S.-based company

User names and passwords represent the keys to the kingdom for malicious attackers. Criminals who know how to penetrate a company's defenses can easily steal hundreds or even thousands of credentials at a time.

A criminal dealing in stolen credentials can make tens of thousands of dollars from buyers interested in purchasing credentials. And by selling those credentials to multiple buyers, organizations that experience a breach of credentials can easily be under digital assault from dozens or even hundreds of attackers..

$1-$8
Typical price range for individual compromised credentials

WHAT CAN AN ATTACKER DO WITH COMPROMISED CREDENTIALS?

- Send Spam from Compromised Email Accounts
- Deface Web Properties and Host Malicious Content
- Install Malware on Compromised Systems
- Compromise Other Accounts Using the Same Credentials
- Exfiltrate Sensitive Data (Data Breach)
- Identity Theft

PROTECTING AGAINST CREDENTIAL COMPROMISE

While there is always a risk that attackers will compromise a company's systems through advanced attacks, most data breaches exploit common vectors such as known vulnerabilities,unpatched systems and unaware employees. Only by implementing a suite of tools including monitoring, data leak prevention, multifactor authentication, employee security awareness training and others - can organizations protect their business from the perils of the dark web.

Carmichael Consulting Solutions, LLC | 11660 Alpharetta Highway, Bldg. 100, Ste. 100, Roswell, GA 30076 | 678-719-9671

The majority of small business owners (six out of 10) report these attacks are becoming more sophisticated and creating more damage with every passing day. With the average cost of recovering from one of these attacks topping out at $3 million, Carmichael Consulting has stepped up to offer a new managed service designed to pinpoint company data, especially PII (personally identifiable information), when it appears on the Dark Web. The New **Dark Web Reporting Solution**, which is available now, is Carmichael Consulting's newest offering in its suite of managed services specifically designed for smaller organizations.

Provides Monthly Bill of Health

Each month, the Dark Web Reporting Solution automatically generates a Bill of Health which flags the confidential information about your company and its top executives that appears on the Dark Web. Best of all, this report features a full scan of activity over a rolling 36 months. You'll know what's out there now and what was out there in the past as well.

Trains Your Staff to Detect Scams

Did you know your employees may be unknowingly helping the bad actors in their quests? One of the latest techniques online scammers use is to send innocent-looking emails with an attachment that appears to be a Microsoft office file. Who wouldn't open that email – especially when it comes from a colleague or trusted partner? Unfortunately, what looks to be an authentic request is really a Trojan. In fact, 48% of malicious email attachments look like Office files. Many of these phishing emails end up in the inboxes of employees in the Account Payable (AP), Payroll and Supply Chain operations. These areas of your company are what nefarious actors consider to be "green fields of opportunity." Perhaps that's why 92.4% of malware comes in through email.

To combat these tricksters, use Dark Web Reporting Solution to create, deliver and monitor internal phishing campaigns based on real-world scenarios. Carmichael Consulting will even educate your staff about how to craft the internal phishing campaigns. These campaigns will teach your employees how to distinguish scammer-sent financial demands from partners' legitimate requests. Until now, small business owners had to worry and wait for an attack they hoped would never come. Now, thanks to Dark Web Reporting Solution, you can know where you stand – each and every month.

Get Dark Web Reporting Solution searching the Internet on your behalf today. Call Carmichael Consulting at **678-719-9671** or visit **www.carmichaelconsulting.net** for more information.