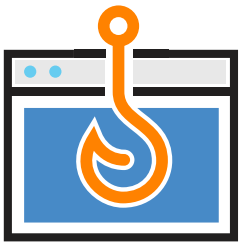
Stolen Credentials: A Problem with No End

What you need to know to combat phishing and brute-force login attacks used to steal sensitive data



Guard Those Passwords or Suffer the Consequences

$1.5 trillion is the size of the cybercrime economy

93% of data breaches begin as phishing attacks

Stolen Credentials Fetch Hefty Sums:

$15 on average;
$60 for military personnel;
$150 for online electronics retail accounts

Thanks to digital transformation, business moves quickly. In fact, we might receive hundreds of emails on any given day. So, doing our jobs requires reading and responding to the emails in our in-box without much scrutiny.

Cybercriminals know this, and use it to their advantage. And while continually entering usernames and passwords to submit and access data may get annoying at times, it's an essential fundamental of cybersecurity. Yet, just as hackers have devised more strategic ways to lure in users, they also now leverage automated tools to increase their odds of breaking into accounts.

Phishing: Firms Increasingly on the Hook for Breaches

Phishing is a social engineering tactic used to steal login credentials and other sensitive information that can then be used to launch more damaging attacks. In fact, as many as 93 percent of data breaches start as phishing attacks.[1] Considering the amount of data stolen and traded on the dark web because of credential theft, phishing's contribution to the global cybercriminal economy—valued at $1.5 trillion—is staggering.[2]

A phishing attack typically starts as an email, text message, shared Google Doc or other common form of digital outreach. Often, the sender poses as a trusted party telling you that you need to verify or update your login information. Hackers who leverage phishing schemes typically cast a wide net with the expectation that someone will click. Alternatively, spear-phishing is a highly targeted form of social engineering. A hacker will research specific targets and then craft a message with an attached file or embedded link that the target has a high probability of opening. Many of these ploys are designed to steal user credentials, while others scheme to trick users into executing malicious files that contain malware.

However, small and midsize enterprises have found that exploits evade intrusion detection systems (66 percent of respondents) and anti-virus solutions (81 percent), according to the Ponemon Institute.[3] Phishing is clearly a top attack vector, and one that shows no signs of leveling off any time soon.

[1] Verizon's 2018 Data Breach Investigations Report
[2] Bromium independent research study
[3] Ponemon Institute

Brute-Force Login Attacks: The Name Doesn't Lie

Brute-force login attacks lack subtlety, to say the least. During such attacks, hackers systematically guess password combinations as they seek to illicitly access privileged information or IT resources. Once they crack the code, they exploit their newfound access for purposes such as data theft or data tampering. Or they may choose to sell the username/password on the dark web, where the average combination goes for $15, and increases to $60 for military personnel credentials and $150 for active accounts of online electronics retailers.[4]

Cybercriminals leverage various attack tools, including automated password crackers that can generate as many as one billion guesses per second. As extraordinary as that sounds, a 10-character pass phrase with letters, numbers and symbols can still take years to crack.

Enter "dictionary attacks." This method tests specific words rather than character combinations, and then adjusts those words with various character combinations that might exist within a password. It may sound tedious, but a hacker only has to succeed once for all the trial-and-error monotony to pay off.

What to Do If Passwords Are Compromised

Point solutions by themselves are inadequate mechanisms for fending off phishing scams. This is partly because there can be millions of networks events on any given day, and tens of thousands of alerts, many of which are false alarms.

Companies must continuously aggregate and monitor log data from their security solutions, and analyze these information streams in real time. The first line of defense in any phishing scheme is to detect malicious files or URLs. Should that fail, the second line of defense is detecting the connection back to the command-and-control server hackers use to run malware or collect login credentials. This requires continuous monitoring of outbound network traffic. Once the phishing threat has been detected, incident responders must work with IT staff to quarantine the infected machine and, if necessary, revoke the stolen login credentials. And that's just for starters.

Bottom line: Putting a stop to credential theft and phishing-introduced malware requires continuous threat detection and response and other capabilities provided by a security operations center (SOC). And while not all organizations have the resources needed to build a SOC from the ground up, there is a cost-effective and compelling alternative: SOC-as-a-service. With highly trained security engineers who monitor network traffic 24/7 and respond to threats in real time, credential compromise is a thing of the past.

Learn more about how SOC-as-a-service improves your organization's ability to preempt the top cyberattack vectors here.

(4) Krebs on Security: The Market for Stolen Account Credentials

ARCTIC WOLF

©2018 Arctic Wolf Networks, Inc. All rights reserved. Arctic Wolf Networks, AWN and the Arctic Wolf Networks logo are trademarks of Arctic Wolf Networks, Inc. in the United States and/or other jurisdictions. Other names used in this document are for identification purposes only and may be trademarks of their respective owners.

SOC2 Type II Certified

Contact us
arcticwolf.com
1.888.272.8429
info@arcticwolf.com