

MITIGATING MODERN THREATS

What the Latest Cybercriminal Gangs Teach Us About Cybersecurity

Richard R. Marsh

Flaherty Sensabaugh Bonasso PLLC

Data insecurity remains a leading threat to businesses and government agencies, and cybercriminals' tactics continue to evolve. Increasingly, these threats come from organized groups based in the United States, Canada, the United Kingdom, and other Western nations, which are often composed of teenagers and young adults whose first language is English. These groups target major corporations and government entities through voice phishing and IT department takeovers. Although they have primarily targeted large corporations such as Caesars Entertainment, smaller companies must remain vigilant, as these methods have filtered down to less sophisticated attackers.

In July 2025, the FBI, the Cybersecurity and Infrastructure Security Agency (CISA), and governmental partners in Canada, Australia, and the United Kingdom issued a joint Cybersecurity Advisory regarding Scattered Spider, a Western cybercriminal group. This group focuses on gaining network access to companies in the telecommunications, retail, healthcare, and airline industries. Scattered Spider's fluid structure was demonstrated in its recent merger with ShinyHunters and Lapsus\$, two similar groups.

Although such groups primarily target large organizations, their methods are easily adapted for use against smaller busi-

nesses. Instructions and exploits shared on Telegram channels and dark web forums allow unaffiliated amateurs to replicate the same strategies locally.

The Cybersecurity Advisory outlines 14 categories of tactics and techniques ranging from reconnaissance and initial access to privilege escalation and data collection. For clarity, these can be summarized into three key phases: (1) Reconnaissance and Resource Development, (2) Methods of Attack, and (3) Takeover.

RECONNAISSANCE AND RESOURCE DEVELOPMENT

Attacks begin with reconnaissance and resource development. Hackers scour company websites and LinkedIn profiles to identify both general employees and IT staff within the organization. They may also rely on leaked or purchased datasets containing personally identifiable information (PII), such as Social Security numbers, birthdates, and family details, to craft precise, targeted attacks. This data allows them to impersonate employees and exploit trust within the organization. Once sufficient intelligence is gathered, attackers move from planning to execution.

METHODS OF ATTACK

Once reconnaissance is complete, attackers deploy phishing, smishing (text-

based phishing), or vishing (voice phishing) to gain credentials. Vishing, enhanced by AI-generated voice cloning, has proven particularly effective at impersonating trusted individuals. Attackers frequently pose as IT staff, persuading employees to install remote-access tools or share multi-factor authentication (MFA) codes.

Although MFA is a critical security measure, attackers have developed techniques to defeat it. One such method is "push bombing." In a push bombing attack, repeated MFA requests overwhelm the user, who eventually accepts one out of frustration—granting the attacker access. Once the request is confirmed, the attacker gains access via the user's credentials.

The groups are also adept at SIM swapping. Cell phones contain a SIM card, either physical or digital, that store the user's account and network information. In SIM swapping, the attacker convinces a mobile carrier to transfer a user's number to a new SIM card, enabling interception of MFA texts and calls.

These attacks rely on layered social engineering. Criminals often call multiple times to learn internal procedures before posing as legitimate IT personnel. Given the wealth of personal information available online, attackers can create credible stories that prompt users to disclose sensitive credentials—leading to system compromise.



TAKEOVER

Once attackers gain a foothold in the organization's system, they may execute a full system takeover using a method known as "Living Off the Land." Rather than deploying malware, they use legitimate administrative tools within the network to collect data and expand control. Because these are legitimate system tools, traditional security software often overlooks the activity.

Attackers frequently create new privileged accounts and even fabricate online personas to reinforce their presence. In some cases, they monitor company communications, including emails, Slack messages, and Teams chats, to detect investigation efforts. They may even join internal calls or threads discussing the intrusion. With this knowledge, the attacker can avoid capture and continue to reside in the system.

PROTECTION AND MITIGATION TECHNIQUES

The Cybersecurity Advisory emphasizes the importance of regular, automated data backups (ideally daily, but at least weekly) with offline storage and routine testing. Organizations should deploy phishing-resistant MFA, apply timely software patches, and enforce robust password policies. CISA currently recommends passwords be at least 16 characters long with a mix of upper/lowercase letters, numbers, and symbols.

Alternatively, users can opt for a passphrase of 5–7 unrelated words. When possible, a password manager should be utilized. Notably, recent guidance advises against frequent password changes, emphasizing strong initial password creation instead.

Access should be strictly controlled, with administrative privileges limited to essential personnel. Application controls can prevent unauthorized software installation, and remote access should be tightly monitored through logging and connection auditing. Users should secure their mobile accounts with carrier-level protections such as SIM locks or PIN codes to counter SIM-swapping attacks.

Because attackers often impersonate IT staff, organizations can implement their own internal codewords for users as an additional layer of identification. They can also require IT staff to contact the user in person or through the phone directory before resetting a password. Even these low-tech measures can prevent significant breaches.

End users are also a source of security. Organizations need to ensure proper user training regarding cybersecurity. The Cybersecurity Advisory specifically recommends diligent employee training against vishing and spear phishing, i.e., targeted phishing.

CONCLUSION

Cybercrime costs the global economy billions of dollars a year. The internet is

full of well-organized cybercriminal groups along with an untold number of amateur hackers working on their own. In response, cybersecurity continues to evolve to defend against these attacks. Companies must implement strong cybersecurity procedures, such as backups and MFA. Moreover, they need to recognize that end users are important to overall security and ensure that the users are properly trained and understand the enormity of the situation. By using resources provided by the FBI, CISA, and others, organizations can strengthen their defenses and reduce the risk of falling victim to this ever-evolving wave of cyber threats.



Richard Marsh is an attorney in Flaherty's Morgantown, West Virginia, office. He has been practicing for more than 15 years, focusing on trust and estate planning, administration and litigation; real property; general business representation; and municipal law. In recent years, he has developed a growing interest in cybersecurity and data privacy issues. Richard is expanding his practice to help clients safeguard sensitive information, manage cyber risks, and navigate the legal implications of data breaches and digital asset protection. He may be reached at 304.225.3057 or rmarsh@flahertylegal.com.