Advisory
Social Engineering: Smishing

Verizon Threat Research Advisory Center (VTRAC)

May 8, 2023

Threat Level Protocol (TLP) (CLEAR)

Executive Summary

The Verizon Threat Research Advisory Center has recently observed a significant rise in smishing attacks against organizations. This threat intelligence advisory delves into the various social engineering techniques employed by cybercriminals and threat actors, with a focus on SMS phishing (smishing). These attacks manipulate individuals, through fraudulent text messaging, into disclosing sensitive information or performing actions that compromise an organization's security. By understanding the tactics and techniques used in social engineering attacks, organizations can better defend themselves and mitigate the associated risks. Verizon offers a comprehensive analysis of smishing techniques and provides recommendations for enhancing security measures.

The Verizon Threat Research Advisory Center (VTRAC) is part of the Verizon Cyber Security Consulting organization and provides threat-related detection, intelligence and response services to Verizon customers.

Key Findings and Impact

Social engineering attacks are a significant and growing threat to organizations due to their reliance on human manipulation rather than technical vulnerabilities. These attacks can have severe consequences, including financial loss, reputational damage, and unauthorized access to sensitive data. Moreover, the success of social engineering attacks can pave the way for more sophisticated threats, such as ransomware attacks.

Smishing Tactics and Techniques in Ransomware Attacks

In smishing attacks, threat actors employ various tactics to manipulate their targets, such as:

1. Context-aware smishing: In ransomware attacks, cybercriminals may use smishing messages tailored to the organization's context or industry. These messages are designed to appear more credible and relevant, increasing the likelihood that employees will trust the content and engage with the malicious links or attachments.
2. Malicious link shorteners: To disguise the true destination of a malicious link, attackers may use URL shorteners to make the link appear less suspicious in the SMS message. When the recipient clicks the link, they are redirected to the malicious website hosting the ransomware payload.
3. Impersonation: Threat actors may use social engineering techniques, such as impersonating a trusted entity or creating a sense of fear and urgency, to manipulate the victim into interacting with the smishing message. For example, attackers may pose as a bank, government agency, or IT support representative to establish credibility and gain the victim's trust.

4. SMS spoofing: Attackers may use SMS spoofing techniques to make their smishing messages appear to come from a legitimate or known sender. This tactic can increase the likelihood that the recipient will trust the message and interact with the malicious content.
5. Curiosity: Attackers pique the victim's curiosity by offering enticing information, such as discounts, promotions, or exclusive news, in the SMS message.

Technique	Description
Initial Access	
Phishing	A broader approach where attackers send deceptive emails or use websites to trick users into providing sensitive information or downloading malicious files. Unlike spearphishing, phishing campaigns are less targeted and may be sent to a wider audience.
Spearphishing Attachment	Attackers send targeted emails with malicious attachments, often disguised as legitimate files, to gain initial access to a victim's system. The victim is prompted to open the attachment, which leads to the execution of the attacker's payload.
Spearphishing Link	Similar to spearphishing attachments, this technique involves sending targeted emails containing malicious links to victims. The attacker aims to trick the victim into clicking the link, which leads to a malicious website or downloads a malicious file.
Trusted Relationship	Threat actors exploit trusted relationships between organizations, employees, or other parties to gain access to sensitive information or systems.
SMS Phishing (Smishing)	Attackers use SMS messages to deceive victims into clicking on malicious links or providing sensitive information. These messages often impersonate trusted entities and exploit a sense of urgency to encourage immediate action.
Voice Phishing (Vishing)	Leveraging voice calls, attackers deceive victims into revealing sensitive information or performing actions that compromise security. The attacker may impersonate a trusted authority to manipulate the victim into following their instructions.
Execution	
User Execution	Attackers rely on users to execute a malicious payload, typically by opening a file or clicking a link. This technique is commonly used in social engineering attacks, as it exploits the victim's trust and curiosity to compromise systems.
Credential Access	
Input Capture	If the social engineering attack is successful in obtaining sensitive information, it may use keylogging or other input capture techniques to obtain credentials or other sensitive data.

Technique	Description
Steal Web Session Cookie	Attackers may use social engineering techniques to trick victims into revealing their web session cookies, allowing the attackers to hijack the victims' online sessions.

Impact of Smishing on Organizations

The impact of smishing attacks on organizations can be severe, including:

1. Ransomware infections: Smishing attacks can be used as an initial attack vector to introduce ransomware into an organization's network. Attackers often use SMS messages containing malicious links or attachments that, once clicked, or opened, act as an initial access vector for a threat actor.
2. Operational disruption: Ransomware infections can cause significant operational disruptions as essential data and systems become inaccessible. Organizations may be forced to halt operations temporarily or resort to manual processes, leading to reduced efficiency, delayed services, and potential loss of revenue.
3. Data loss: In some cases, organizations may be unable to recover encrypted data, either because they refuse to pay the ransom or because the decryption process fails. This data loss can have long-term consequences, including the loss of critical business information, intellectual property, or sensitive customer data.
4. Financial impact: Ransomware attacks can result in substantial financial losses for organizations, including the cost of paying the ransom, expenses related to system recovery and remediation, and potential revenue loss due to operational disruptions or damage to the organization's reputation.
5. Reputational damage: Organizations affected by ransomware attacks resulting from smishing may suffer reputational damage, leading to a loss of customer trust and potential business. Public disclosure of the incident or media coverage may amplify the negative impact on the organization's image.
6. Legal and regulatory repercussions: Organizations that fall victim to ransomware attacks due to smishing may face legal and regulatory penalties, especially if they fail to protect sensitive data or comply with data protection regulations. This can include fines, sanctions, and potential lawsuits.

Recommendations

To defend against smishing attacks, organizations should implement a combination of security measures and best practices, including the following recommendations and security controls:

1. Security awareness training: Regularly conduct security awareness training for employees, emphasizing the importance of verifying the legitimacy of SMS messages, recognizing common smishing tactics, and being cautious when clicking on links or providing sensitive information.
2. Reporting and incident response: Establish a clear process for reporting and handling suspicious SMS messages, including smishing incidents. Encourage employees to report any suspected smishing messages to the appropriate personnel and ensure your incident response team is prepared to investigate and remediate any potential security breaches.

3. Endpoint protection: Implement robust endpoint protection solutions, such as antivirus and anti-malware software, on all devices within the organization. Ensure these solutions are regularly updated to protect against the latest threats.
4. Mobile device management (MDM): Deploy a mobile device management solution to enforce security policies on employee devices, restrict the installation of unapproved apps, and apply necessary security patches and updates.
5. Network segmentation: Segment your organization's network to limit the potential spread of malware introduced through smishing attacks. By isolating critical systems and data, you can reduce the impact of a successful attack.
6. Regular backups: Maintain regular backups of critical data and systems to ensure a quicker recovery in the event of a ransomware infection or data loss resulting from a smishing attack. Store backups offline or in a separate, secure location to prevent unauthorized access.
7. Multi-factor authentication (MFA): Implement multi-factor authentication for accessing sensitive systems and applications to reduce the risk of unauthorized access due to compromised credentials obtained through smishing attacks.
8. URL filtering and reputation services: Use URL filtering and reputation services to block access to known malicious websites or domains associated with smishing attacks. These solutions can help prevent users from inadvertently visiting phishing websites linked in smishing messages.
9. SMS gateway security: Implement security measures at the SMS gateway level, such as content filtering and sender validation, to reduce the likelihood of smishing messages reaching your employees.
10. Security audits and vulnerability assessments: Conduct regular security audits and vulnerability assessments to identify potential weaknesses in your organization's security posture and address any identified issues proactively.

By implementing these recommendations and security controls, organizations can significantly reduce the risks associated with smishing attacks and better protect their employees, data, and systems from potential compromise.

Customers of Verizon cybersecurity services are reminded that they may engage Verizon’s security consulting services to conduct a detailed assessment of their networks. This preventative due-diligence review will help to identify and mitigate any possible malicious activities affecting critical services that can result in data loss and system integrity. For more information or further assistance, please contact your Verizon account representative or designated service liaison.

verizon✓

Proprietary & Confidential Statement: This document and the information disclosed within, including the document structure and contents, are confidential and the proprietary property of Verizon and are protected by patent, copyright and other proprietary rights. Any disclosure to a third party in whole or in part in any manner is expressly prohibited without the prior written permission of Verizon.