PUTTING FEDERAL SECURITY CONTROLS TO THE TEST

How a CISA red team assessment proved one agency's hardened network was still vulnerable to phishing attacks and credential theft.

> A Scoop News Group Report

On February 23, 2023, the Cybersecurity and Infrastructure Security Agency (CISA) released a report from a red team assessment they conducted in 2022 "at the request of a large critical infrastructure organization with multiple geographically separated sites."

According to the report, "the team gained persistent access to the organization's network, moved laterally across the organization's multiple geographically separated sites, and eventually gained access to systems adjacent to the organization's sensitive business systems (SBSs)."

By the time they reached the end of their assessment period, MFA prompts prevented them from accessing one SBS, and they were unable to complete a plan to compromise the second SBS.

In a real-life scenario, a threat actor would not face similar time constraints to gather information and move throughout the network and could have maintained their access for an unknown amount of time. The assessment found that the organization did not detect the red team's activity throughout the assessment, "including when the team attempted to trigger a security response."

The initial access was gained through spearphishing emails — also known as business email compromise (BEC) — which targeted specific users in the organization. The team sent tailored emails to seven targets using commercially available email platforms. After building a rapport with the individuals, the "attackers" led them to accept a virtual meeting invite which steered them to a red team-controlled domain with a button that, when clicked, downloaded a "malicious" ISO file. After the download, another button appeared, which, when clicked, executed the file.

Of the seven targets, two responded to the phishing attempt, giving the red team access to two workstations on different site locations.

"There are a lot of different ways threat actors can get that initial access," shared Garrett Guinivan, solutions architect and threat analyst at Proofpoint. "And often what leaders don't realize is the high number of threats coming in via email. When you look at the big piece of this red team advisory, once the attackers had access, they were able to move laterally, establish persistence and work towards their objectives."

The dangers of phishing tactics

Malicious actors continuously refine their attacks and look for new ways to trick users into giving up valuable information or bypass defenses. Identity-focused attacks strategically recognize that people are the most vulnerable entry point to an organization, through

"Having accurate data of where your biggest threats are, and your true threat model, are ways we can help executives better understand where they need to invest their security resources."

- Garrett Guinivan
Solutions Architect and Threat Analyst, Proofpoint

no fault of their own, but simply because technology can only go so far in defending an organization's resources.

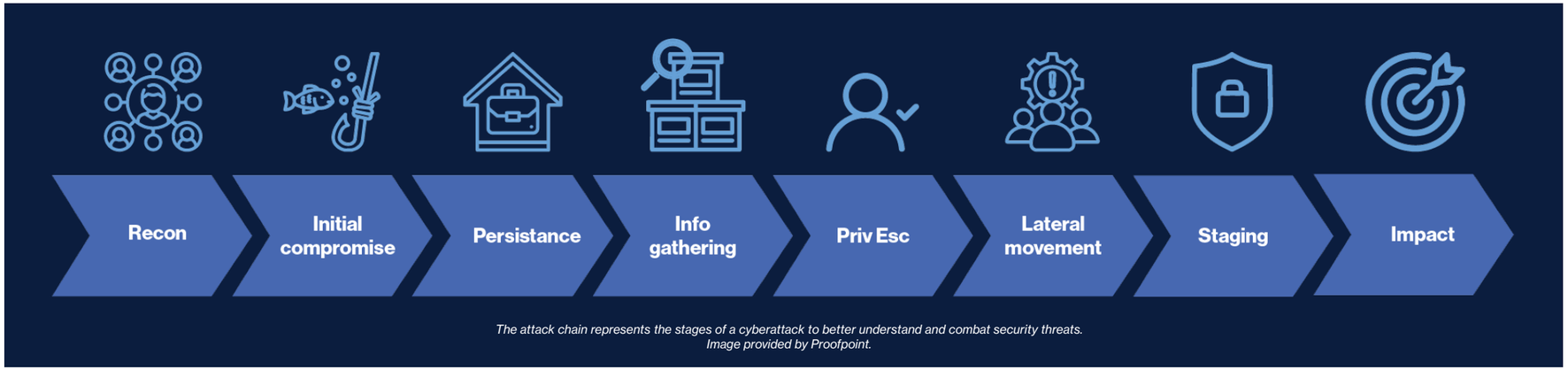
Social engineering techniques that exploit human fear and error provide a valuable tool in a threat actor's arsenal. According to Proofpoint's 2023 State of the Phish report, phishing techniques such as telephone-oriented attack delivery (TOAD) and multifactor authentication (MFA) phishing have recently added disruptions to the threat landscape. All the while, BEC continues to be a highly lucrative form of cyberattack.

"What all these attacks have in common is they target people. So even as we see an emphasis on zero trust to combat security weaknesses, attackers are leveraging that framework in their own build-up and their growth and maturity of attack models which use phishing to go after credentials," said Hanna Wong, director of public sector solutions at Proofpoint.

While organizations continuously evolve their security strategies to combat these attacks, Wong said government agencies remain at a disadvantage in the fight. Federal security compliance mandates and frameworks are all public, allowing adversaries to learn and adapt their techniques in-line with an agency's ability to implement the required changes.

"What any government agency across the board should be asking themselves, despite having a mature security stance and being hardened, is it enough?"

- Hanna Wong
Director of Public Sector Solutions
Proofpoint



The attack chain represents the stages of a cyberattack to better understand and combat security threats. Image provided by Proofpoint.

"What any government agency across the board should be asking themselves, despite having a mature security stance and being hardened, is it enough?" Wong added. "Are you continuing to progress, grow and assess your cybersecurity posture, or are you just meeting the necessary compliance requirements?"

Defending at all stages of the attack chain

"One of the most surprising findings from the red team assessment was that once they infiltrated the network, the organization never received any alerts that a malicious actor was inside, allowing the team to gather as much intel as they could," said Guinivan.

It is helpful to conceptualize where security gaps may reside if leaders breaking down an attack chain into its eight stages to ensure they have a playbook and alerts properly sent to defend their network through an attack cycle.

In the first two stages, an attacker will recon a network to find the initial point of compromise. While there are many ways to get into a network, phishing techniques — such as TOAD, BEC and MFA phishing — are the most widely used tactics so educating users on phishing tactics is a strong line of defense.

But once an attacker has access, many organizations don't have the tools to alert them that they are inside their environment. The danger here is that an attacker can maintain persistence in the network, gather information, escalate their privileges and move laterally

across the network until they are ready to launch their attack.

This is where establishing identity threat, detection and response (ITDR) practices can be helpful. ITDR focuses on detecting and preventing credentials and privilege account abuse from vulnerable identities in an organization. ITDR also deploys honeypots for early detection of an attack, giving defenders an edge in learning more about a threat actor's techniques.

"ITDR platforms like Illusive, Proofpoint's new acquisition, make it harder for an actor to move inside a network and provide an organization with both the visibility of risks

that need to be remediated, in addition to providing alert mechanisms that make it harder for attackers to maintain a persistent presence or escalate their privileges," explained Guinivan.

Training as a security tool

Technology can only take an organization so far. Social engineering attacks are successful because they exploit our human weaknesses. That is why awareness-through-training is critical in further closing security gaps.

"Proofpoint gathers data of all the attacks we are blocking, and who is being targeted within an organization. And we take these real-world examples to create training for specific profiles within an organization," said Wong. "These are people that if they click on something or they send an invoice, it's going to be a bad day for the organization. And it isn't always your executive levels, it's anyone who has access."

Wong explained how Proofpoint takes real-world examples of ways that people are being targeted, because not everyone is targeted at the same level. "Organizations tend to put more resources on executives, but it's really anyone who has access to anything because threat actors count on privilege escalation techniques to work in their favor," she said.

This type of data-focused training is aimed at changing user behavior so that organizations can help their employees improve their security awareness based on the threats they are facing daily.

Staying ahead of the adversary

Cybercriminals are thinking outside of the box as they craft attack techniques, and security defenders need to take a similar stance.

"At Proofpoint, we see identity and credential theft as one of the biggest security risks, which is also what the CISA red team report focused on. The red team was forced to focus their effort on identity theft by phishing as the 'malicious actor' to gain initial access because the team was unable to find easily exploitable network access points," shared Guinivan.

"Proofpoint has reported on a number of MFA phishing attacks that are being used today to steal tokens. Evilginx2, Modlishka, EvilProxy, there's a lot of names, but it really comes down the fact that threat actors have even more tools to bypass MFA," he said.

And while the federal government tends to focus more on advanced persistent threats (APTs), Guinivan explained that threat data Proofpoint is collecting on attacks against federal and public sector agencies, compared to a finance or healthcare organization, show credential phishing threats still make up 70-to-80% of the entire landscape.

"Having accurate data of where your biggest threats are, and your true threat model, are ways we can help executives better understand where they need to invest their security resources," he said.

Wong added, "cyberthreat actors are getting more creative with their attacks on people and using modern tools to obfuscate their activity. So it is incredibly important that federal leaders integrate security solutions that are impactful, and take the agency beyond meeting minimal compliance."

Learn more about integrating solutions that protect people and data from the latest cyberattacks.

This report was produced by Scoop News Group, for FedScoop, and underwritten by Proofpoint.

FEDSCOOP | proofpoint.