SOPHOS

Combatting Evolving TTPs: Expert Strategies for Government and Education

As technology continues to advance, so do the threats that we all face. Cybercriminals are constantly developing new tactics and techniques, and it can be daunting just to keep up.

In today's rapidly changing threat landscape, it's more important than ever to be proactive when it comes to cybersecurity. By being alert to the latest cybercrime TTPs — Tactics, Techniques, and Procedures — IT and security professionals can build stronger, more effective defense strategies.

A Sophos Whitepaper. May 2023

Concerns for the public sector

The public sector faces a number of cybersecurity challenges. The following security issues demand the most urgent attention.

An Increased Attack Surface

The post-Covid shift to remote work has expanded the attack surface for organizations everywhere. Along with the rise in cloud services, the Internet of Things (IoT), and mobile devices, this has created a new battleground for cyber adversaries to exploit. And since many public sector organizations still rely on outdated technologies, they're more susceptible to today's cyberattacks.

A Lack of Cybersecurity Resources

The shortage of skilled cybersecurity professionals makes it difficult to have the right personnel in place to effectively manage cybersecurity efforts. This is made more complicated as the public sector often struggles to compete with the salaries offered by the private sector for top-tier security talent. Staff who do sign on face the added pressure of juggling multiple projects and responding to complex incidents simultaneously, which can lead to burnout and alert fatigue.

Significant Budgets Shortfalls

We all know that securing technologies and staff that are up to the task can be expensive. And the limited budgets of many public sector organizations make it difficult to secure every endpoint, upgrade or replace outdated technologies, or hire personnel qualified to combat today's cyber threats. Unfortunately, this leaves these organizations vulnerable to the mercy of their adversaries.

Understanding the attack landscape

Even with limited budgets and a shortage of skilled professionals, public sector organizations must remain aware of the latest tools, techniques, and practices (TTP) that pose the greatest risk to their operations. By identifying these risks, municipalities, agencies, schools, law enforcement, and other public sector entities can prioritize their defenses against the most critical threats. This approach can make network security and cybercriminal detection and response less overwhelming and more targeted, allowing organizations to focus resources where they'll have the most impact.

Using the MITRE framework as a guide

The MITRE ATT&CK framework is a versatile tool that organizations and security teams can use to analyze threat intelligence, identify security gaps, and prioritize security investments. Think of it as a globally-accessible knowledge base of adversarial tactics and techniques based on real-world observations — a framework for understanding and defending against new and emerging threats that are constantly evolving.

As attackers are quick to adjust their tactics, staying up to date on the most relevant threats is an ongoing necessity.

So, what are the latest cybercrime TTPs? And how can public sector defenders stay one step ahead? Let's take a look.

Fortifying defenses: Protecting your organization from the top 3 TTPs.

TTP #1 — PHISHING

As the top form of cybercrime, phishing is often the first tactical point of entry into an organization's network. Spear-phishing, spam, and other social engineering attacks relentlessly target end-users, and the techniques adversaries are deploying are becoming more and more advanced. Even the most experienced employees can have difficulty detecting these attacks.

What's needed to defend against current and future phishing attempts:

- **Be vigilant about security awareness.** Rather than relying on the mandated one-and-done annual training, organizations should invest in ongoing programs that educate and empower employees to recognize and report potential threats. This approach can significantly reduce an organization's likelihood of being phished.
- **Update software and apply patches.** Attackers look for the easiest way in and look for known vulnerabilities. Keeping software and systems up-to-date closes those entry points, makes the attack too much trouble, and sends the adversary searching for another target. With regular patches and updates, organizations stay protected against future threats.
- **Employ an extra layer of protection.** By requiring a second form of identification, such as a fingerprint or a code sent to a mobile device, two-factor authentication (2FA) can help prevent attackers from gaining access to sensitive data even if they successfully phish an employee's credentials. For more robust protection, consider using a hardware token as part of your 2FA process.

TTP #2 — REMOTE SERVICE ATTACKS

Remote services, especially in the age of BYOD, have become a vulnerable entry point for cybercriminals to access your network. Without proper security measures and technologies in place to prevent these tactics — which are often taking place further down the attack chain — cybercriminals can easily penetrate public sector networks through remote services, often remaining undetected.

How to safeguard against remote services attacks:

- **Limit account access.** To minimize the risk of unauthorized access to sensitive systems and data, implement control policies that restrict access to only those who require it. One effective method is role-based access control (RBAC), widely used in government agencies and industries where access to sensitive information is strictly regulated. RBAC allows admins to assign roles and limit resource access to only what's necessary for that specific job.
- **Start the zero trust journey.** Zero trust is a comprehensive strategy based on the principle of "never trust, always verify." It addresses the challenge of granting appropriate application access to authorized users and devices while minimizing network vulnerabilities. It is not a one-size-fits-all solution or a single product; rather, it consists of multiple layers of defense that restrict lateral movement within your network. To establish a solid foundation, begin with identity management, employing a combination of multi-factor authentication (MFA) and access policies. For a more advanced layer or protection, consider adopting a ZTNA gateway which enables more precise control by granting access to individual applications based on the user's identity, context, and policy compliance.
- **Strengthen email security.** You probably already have an email filter in place but consider implementing deep packet inspection (DPI), a technique that examines the contents of data packets as they pass through a network. DPI can identify and block malicious traffic, including malware and phishing attempts, making it a valuable addition to your existing email filtering solution.

TTP #3 — SUPPLY CHAIN COMPROMISE

Do you depend on third-parties to handle essential business functions, like IT infrastructure, finance, and business operations? Allowing these vendors to connect to your network can increase your vulnerability to supply chain attacks, a common tactic adversaries use to gain access to your environment and initiate malicious activities such as data theft, extortion, and ransomware.

What's needed to protect against supply chain compromise:

- **Vet vendors for risk management.** The best defense is knowing who you partner with and how they approach security. To effectively manage vendor risk, conduct a cybersecurity audit of each vendor relationship by evaluating their security practices, the type of data they can access, and their level of access to your systems. If you have limited resources, start with a short survey or questionnaire to identify security protocols and build from there.
- **Lockdown vendor access.** Many organizations use single sign-on (SSO) — which can provide access to multiple systems with one set of credentials — so consider restricting vendor access to only the systems necessary for their specific tasks. To further secure your network, require the use of MFA and/or zero trust, which will prevent unauthorized access if credentials are compromised, and enforce this mandate in contracts and vendor agreements.
- **Early detection minimizes impact:** To spot early signs of compromise across your vendor network, consider implementing next-gen AI technologies and telemetry. There are two paths to take: invest in the necessary technology and training to hunt for anomalies in-house or hire a managed detection and response (MDR) service provider to monitor things on your behalf.

Cybersecurity-as-a-Service: Staying ahead of cybercrime TTPs

As cybercriminals refine their tactics, anticipating and mitigating the latest threats can feel impossible. But you don't have to go it alone.

Sophos offers a proven approach to threat prevention with Cybersecurity as a Service, providing organizations in the public sector with a range of benefits, including elevating cyber defenses, freeing up IT capacity, and adding expertise without adding headcount.

Whether you want to fully outsource your threat hunting or supplement in-house services, Sophos can help improve your cybersecurity ROI while providing you with 24/7 peace of mind.

To learn more about how we can help your organization stay one step ahead of cybercrime, **speak with a Sophos partner** or **connect with a Sophos expert today**.

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

2023-06-27 (WP-PC)

SOPHOS