POLSINELLI

Publications

February 26, 2025 • Updates

Threat Actor Trends and Practical Guidance —A Conversation Between Polsinelli and Coveware

As cybersecurity professionals know all too well, threat actors continue to evolve in order to overcome organizations' defenses. However, by analyzing these threats and trends, organizations can take steps now to further reduce their risk and to better prepare to respond when an incident occurs.

Coveware is a leading cyber extortion incident response firm that helps victims recover encrypted or stolen data as a result of a cyberattack. Polsinelli and Coveware have partnered for many years in helping organizations of all sizes and industries navigate cyber extortion and ransomware attacks. To help organizations prepare for the upcoming year, Polsinelli spoke with Coveware regarding threats and trends observed in 2024 and predictions for 2025. Based on these threats and trends, organizations can take steps to further reduce the risk of incidents and to better prepare to respond to an incident if one occurs.

There is little, if any, data indicating that certain industries are more at risk than others for a cyberattack. Accordingly, all businesses continue to be at risk and should prepare for when (not if) a cyberattack will happen. All organizations should follow a layered approach to address this risk:

- Reducing the risk of an incident through risk assessments, technical security measures, training and vendor vetting;
- Reducing the scope of a potential incident through record retention and deletion policies, data mapping and segmentation;
- Preparing to effectively respond to an incident with updated and exercised incident response plans.

Although all entities are at risk for a cyberattack, the type of attack and the root cause of the attack can vary by entity size. Threat actors continue to exploit known software vulnerabilities to infiltrate small and medium-sized businesses. The threat actors can easily identify organizations that are vulnerable to these attacks, and smaller organizations often lack sophisticated patching programs that address the frequent patches and updates necessary to address this risk. Threat actors are also likely to

Related People

- Alexander D. Boyd
- Jessica L. Peel

Related Capabilities

- Privacy & Cybersecurity

continue both exfiltrating and encrypting data during a ransomware attack on a small-to-medium-sized business.

In contrast, threat actors are increasingly choosing to steal data from larger organizations without also encrypting the data in the attack in order to further delay detection and to reduce their profile with law enforcement. Threat actors are also more likely to invest in more sophisticated social engineering attacks for these larger organizations. While large businesses often implement employee training to identify traditional phishing emails, threat actors are now leveraging artificial intelligence to launch more sophisticated and targeted attacks using advanced data analytics coupled with highly convincing voice phishing ("vishing") schemes.

For example, a threat actor may call an employee from a spoofed number, appearing to be from a member of the IT department, regarding a network problem or routine maintenance project, then confirm the name of the employee's manager and ask the employee to perform a simple task over the phone. During that task, the threat actor is granted access to the employee's computer and is able to install malware for remote access, move laterally within the environment, steal data or otherwise cause damage. Organizations should ensure that their training programs include multiple avenues for phishing, including email, text and phone calls.

Both large and small organizations are also increasingly falling victim to search engine optimization (SEO) poisoning or "malvertising" where the threat actor has tricked an employee (even an IT professional) into downloading and installing malicious software designed to look like a known legitimate tool. They achieve this by registering domains to host malicious payloads and increasing the prominence of such domains so they appear high up in the list of search engine results, thereby feigning credibility and authenticity. Organizations should ensure that internal and external IT personnel are using only vetted tools from approved sources. Threat actors also continue to specifically target external managed service providers (MSPs). Organizations should appropriately vet all vendors, including MSPs, and ensure that their contracts address cybersecurity requirements and data incident notifications and responsibilities.

"Phantom demands" also increased for all businesses in 2024, and it is expected they will continue to take place through 2025. A phantom demand occurs when a threat actor claims to have infiltrated an organization's network and/or stolen an organization's data but has not actually done so. Threat actors typically provide phantom demands via email, and they fall into two main categories:

- An entity was not actually attacked, and the threat actor makes a low monetary demand with the hope that payment will be made without due diligence.
- The entity or a third party that holds the entity's data experienced a data security event within the preceding several years, and the threat actor discovered stale information from those incidents on the dark web.

The first type of phantom attack has been occurring for years; however, the second type (the legacy extortion event) is becoming more frequent. We believe this trend is the result of combined circumstances, including a shrinking victim landscape, increasingly desperate economics for extortion actors and the availability of artificial intelligence to easily data mine large datasets from prior incidents.

Lastly, between 2023 and 2024, federal and international law enforcement made significant progress in investigating, identifying and disrupting large ransomware groups, their ecosystems and their resources. As a result, market share is no longer held by two to three large ransomware-as-a-service (RaaS) syndicates. Instead, the landscape is

populated by a few legacy groups that strive to maintain a small footprint, a handful of "new" variants that have emerged following the collapse of others, and a decentralized collection of lone actors who likely came from prior RaaS organizations but have struck out on their own now that being linked to a group appears to carry more risk than reward compared to years past. These newer groups and lone threat actors often act in less predictable ways following an attack. This means that organizations may have less information available to them during communications with the threat actor. For example, there will be less information known about whether the threat actor will actually provide a decryption key in exchange for payment, whether the threat actor will negotiate and whether the threat actor will still publish leaked data even after payment is made. Decryption tools from smaller groups can also be less reliable. As a result, it is even more important for organizations to do everything they can to reduce the risk of an attack and to ensure that they have recent, viable backups if an attack does occur.

While no organization can prevent all potential cyberattacks, a comprehensive cybersecurity, resiliency and incident response program can reduce the risks associated with these attacks. By analyzing and forecasting threat actor trends, organizations can put themselves in the best position to address these evolving risks.