The cyber threat landscape part 3: Evolving attack techniques and tactics

BY INTIGRITI · NOVEMBER 21, 2024 · LAST UPDATED ON APRIL 28, 2025

As cyber attackers refine their skills, their methods evolve to exploit vulnerabilities in innovative and increasingly difficult-to-detect ways. The modern cyber threat landscape includes new attack vectors, rapid weaponization cycles, and strategic targeting, making it essential for organizations to stay informed and ready to adapt. This part of our cyber threat landscape series explores the advanced tactics used by threat actors today and why these tactics demand a forward-looking approach to defense.

Modern attack techniques: Going beyond the basics

Today's attackers use multi-faceted approaches, combining technical expertise with psychological insights and leveraging the vast online marketplace of malicious tools. Understanding how these techniques work can reveal crucial vulnerabilities and illuminate the need for adaptive cybersecurity strategies.

1. Supply chain compromise: Attacking indirectly

Supply chain attacks target indirect entry points through third-party vendors, suppliers, and service providers. These attacks are highly effective - inserting malware into a routine software update, infiltrating thousands of organizations without their knowledge. Because they compromise trusted networks, supply chain attacks are often undetected until significant damage is done.

2. Ransomware-as-a-Service (RaaS): Lowering the barrier for entry

Ransomware has become more accessible through Ransomware-as-a-Service (RaaS) models, where developers sell or lease ransomware tools to less technically-skilled cybercriminals. This model has led to a spike in ransomware attacks, as even minor actors can now leverage sophisticated encryption-based attacks. With RaaS, the threat is compounded as attack techniques can be replicated and executed widely, contributing to significant financial and data loss across sectors.

3. Exploiting zero-day vulnerabilities: Speed and scale in weaponization

Zero-day vulnerabilities—flaws that are unknown to software vendors—are critical openings for attackers who aim to exploit them before patches are available. The bad news is, they are on the rise. Threat actors today can operationalize attacks within hours of a vulnerability's discovery, often weaponizing it at an unprecedented scale. The 2021 Log4j vulnerability was a striking example of rapid weaponization, underscoring the urgency for agile, real-time defense strategies to counteract these attacks.

4. Advanced social engineering: Phishing in 3D

Social engineering has evolved into a far more complex tactic, where attackers leverage detailed personal and organizational information to manipulate employees. These advanced phishing campaigns may involve impersonating trusted parties like C-suite executives or IT staff. With tactics ranging from business

email compromise (BEC) to voice phishing (vishing), these campaigns aim to exploit human vulnerabilities and bypass technical safeguards.

Real-world example: TAG-112's sophisticated cyber campaign

A recent investigation exemplifies how advanced tactics are employed in real-world scenarios. Chinese state-sponsored threat group TAG-112 **compromised two Tibetan websites**, Tibet Post and Gyudmed Tantric University, to deliver the Cobalt Strike malware. The attackers embedded malicious JavaScript in these sites, spoofing a TLS certificate error to trick visitors into downloading a disguised security certificate. Once downloaded, the malware enabled remote access and post-exploitation activities.

This incident showcases how state-sponsored threat actors leverage advanced tools like Cobalt Strike and exploit vulnerabilities in widely used platforms such as Joomla. TAG-112's infrastructure also incorporated sophisticated obfuscation tactics, such as using Cloudflare to hide its servers' IP addresses, making attribution and mitigation significantly more challenging. Such cases highlight the necessity for organizations to adopt proactive defense measures to counter evolving cyber threats.

Defensive measures against advanced tactics

Evolving tactics require evolving defenses. Organizations today must use a blend of proactive and reactive security measures to keep up with the speed and scale of modern cyberattacks.

Utilize threat intelligence and collaboration

Staying informed about new vulnerabilities and emerging threats is critical. Threat intelligence services and industry partnerships allow organizations to keep up with shifting tactics, share indicators of compromise (IOCs), and deploy preemptive defenses. Collaborative approaches can help detect trends that individual companies may not notice alone.

Bug bounty programs for real-time defense

Bug bounty programs empower organizations to identify and address vulnerabilities before they can be exploited. By tapping into a global pool of ethical hackers, organizations can simulate real-world and continuous testing of digital assets, uncovering potential vulnerabilities that internal teams might overlook.

Adopt zero trust principles

A zero trust approach assumes no user or system is inherently trusted. With the rise of insider threats and supply chain vulnerabilities, this approach helps ensure that all network access is authenticated, authorized, and continuously validated, regardless of the user's location or device.

Conclusion: staying proactive amid evolving threats

In the face of fast-evolving cyber tactics, a proactive, layered defense is not just advisable—it's essential. By staying informed about emerging techniques and adopting strategies like threat intelligence, bug bounty programs, and zero trust, organizations can adapt to the dynamic threat landscape. The next

installment in this series will dive into the role of emerging technologies in cybersecurity and the new risks they may introduce.

In the meantime, if you'd like to learn more about bug bounty and if it's right for your organization, talk to one of our team today.

REQUEST A DEMO	VISIT THE WEBSITE	GET IN TOUCH
intigriti.com/demo	intigriti.com	hello@intigriti.com