How are Threat Actors Leveraging Access in the Enterprise?

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled, “How are Threat Actors Leveraging Access in the Enterprise?” on July 20, 2022.

Last month the ACF examined the tactics, techniques and procedures threat actors deploy to gain access to the enterprise. This session, in response to member feedback, raised issues such as the the porousness of Active Directory, compromised web applications, the risks of lateral cloud movement over compromised privileged accounts, threat hunting best practices and governance.

This roundtable was conducted under the Chatham House Rule: ACF members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers, nor participants, is revealed.

"Every threat is an insider threat"

“Gone are the days when everyone believed that hardening the enterprise would keep out the bad guys,” said a subject-matter expert. “The threat actors have shown us we can never harden enough. But we can deter and disrupt them once they’re inside.” The conclusion: More mature enterprises also protect inside the computing environment, not just the perimeter.

Disrupting the threat actor business model

Because most threat actors are financially motivated, they are seeking the greatest return with minimal effort. Enterprises can use this mindset to their advantage. One CISO endorsed the strategy of “delay and disrupt to give us time to detect.” Thus, if threat actors can be discouraged when they encounter indications of cybersecurity maturity, they may well decide to move on to a different victim.

After the call, a subject-matter expert provided more detail about one tool used to detect intrusions: “HoneySPN is essentially a fake Active Directory domain account tied to a Service Principal Name (SPN). If auditing within Active Directory on the account is configured properly, then attackers attempting to kerberoast (https://attack.mitre.org/techniques/T1558/003/) a domain will query the HoneySPN and trigger the alarm. The key here is to make the honey account look as legitimate as possible while making sure it cannot be leveraged against you, so you’ll want to take care to neuter its privileges and set an uncrackable password. HoneySPNs are a quick way to detect one of the most common escalation paths attackers choose.”

Vulnerabilities of legacy systems

For all the talk about security in the cloud, subject-matter experts said greater risks reside in legacy systems that allow threat actors to make first-time connections and then move laterally across the computing environment. “There is a common misconception that threat actors will focus on attacking the cloud perimeter, but actually they attack legacy systems first and then pivot to the cloud or hybrid cloud.”

Several Forum members cautioned about focusing on new tools at the expense of overlooking systematic legacy system hygiene. A board member said boards should be asking the question: “Are we making it harder for threat actors by getting rid of older technologies?”

Governance and the cost of compliance

Forum members had much to say about governance and maintaining enterprise-wide alignment on cybersecurity budget, policies and authority, including:

- “Make sure your governance model adapts to current conditions. It shouldn’t be static.”
- “We have found it useful for the CISO to report to the general counsel because in our industry cybersecurity is tied in with legal requirements and regulations.”
- “Governance should be about holding people accountable.”
- “More money in the cybersecurity budget is not necessarily a recipe for success. Once the security organization gets too big, people start assuming that security is not their problem and compliance becomes an issue.”
- Security needs to be part of the entire business, a business-level priority and a way by which we measure ourselves as an organization.”

Leading practices

- **Assume threat actors have your insider information.** One CISO said they operate under the assumption that they are being breached all the time and focus on the speed in which they can detect and respond to breaches.
- **Adopt an adversarial mindset.** Secure the tools by which threat actors can try to onboard as an employee–job aids, network diagrams, notes on devices or internal wikis. Analyze day-to-day processes and how they can be compromised.
- **Harden credentials.** Evaluate access profiles for weaknesses. Set a strong password policy and monitor them to ensure that they remain strong.
- **Monitor specific indicators,** including anomalies in traffic volume and outbound traffic from the host network to outside networks, as well as and first-time connections. Be proactive about hypothesis-based testing. Deploy automated detection and response to gather endpoint data.
- **Drive home the importance of security within the DevOps team and business users.** Don’t let tight delivery deadlines become an excuse for not addressing cybersecurity

upfront. Enlist business support in identifying suspicious activity by letting them know what questions need to be asked.

- **Network segmentation is critical,** particularly across legacy systems. Just because it's one of the basics doesn't mean should be overlooked.
- **Reconsider the economics of making exceptions.** When business leaders, for example, push back on security fundamentals, invariably the enterprise will be forced to spend more money. "The cost of backing up exceptions can add millions to your operating costs," said a subject-matter expert.

CONTACT

Kris Burkhardt

Accenture Chief Information Security Officer

Accenture Cybersecurity Forum Chair

LinkedIn

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 710,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at accenture.com.

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us on @AccentureSecure on Twitter or visit us at www.accenture.com/security.

View the entire suite of ACF roundtable summaries on our webpage – here.