How are Threat Actors Getting into the Enterprise?

The Accenture Cybersecurity Forum (ACF) recently convened a virtual roundtable titled, “How are Threat Actors Getting into the Enterprise?”

. In this session, Forum members and subject-matter experts shared insights on threat actor tactics, techniques and procedures (TTP) and remediation steps cybersecurity teams should prioritize in response.

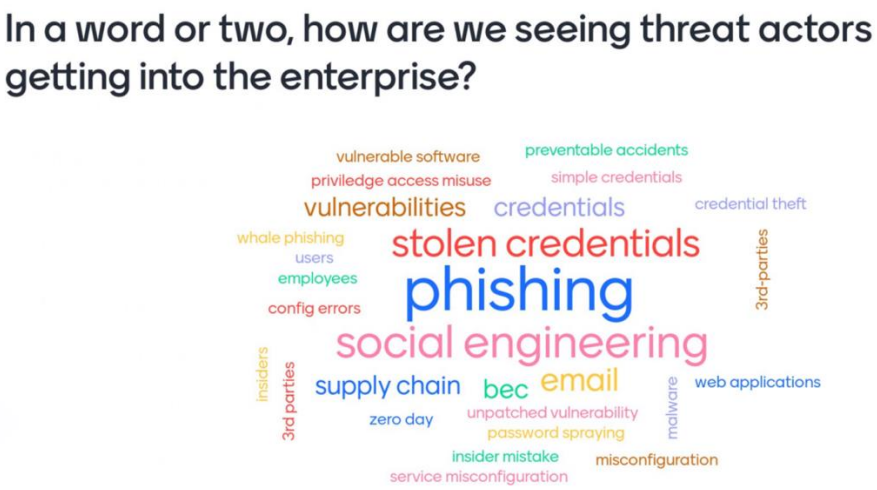
This roundtable, held on June 21, 2022. was conducted under the Chatham House Rule: ACF members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers, nor participants, is revealed.

Below is a brief summary of the call:

Threat actor TTPs

Forum members most frequently identified long-standing threat TTPs such as phishing, stolen credentials and social engineering as the most common ways of entering the enterprise. These practices have been common for years but continue to pose a threat.

Looking ahead, new technologies will present new threat vectors, with threat actors expected to become increasingly creative and flexible in their approaches. A subject-matter expert said threat actors are getting more skilled and knowledgeable and are making greater use of the native tools and capabilities we’re providing them on our extended operating systems, learning about vulnerabilities from public sources, leveraging commoditized attack tools, deploying drive-by downloads of malware and conducting zero-day and supply chain attacks.



Vulnerabilities that require special attention

Threat actors may attack in different ways, but they still have a mission to invade Active Directory and other crown jewel assets, said a subject-matter expert. With this in mind, Forum members discussed several scenarios that can put their enterprises at risk. For example, one CISO described risk associated with user account provisioning—the lag time between when a new hire is issued preliminary credentials and when multi-factor authentication is established. "Remote connectivity from day one for new hires and the time it takes them to set up multi-factor authentication (MFA) creates real challenges," the CISO said. "We had to re-evaluate how soon we create credentials for new employees."

Another Forum member pointed to the value of CISA Vulnerability Directives. While those directives require all federal civilian executive branch agencies to take remediation actions, the information can also apply to other enterprises. Yet another Forum member raised the issue of vulnerabilities in the Slack messaging app.

Dark Web risks

Threat actors scan the network access market, looking for people who have accessed a phishing link that has compromised devices. "A threat actor can go into a search bar and look for all the compromised devices in a particular enterprise," said a subject-matter expert. They are also exploiting back channels, like Slack, for indirect access to enterprise assets. In a recent case, a threat actor succeeded in that by using a $10 bot, the subject-matter expert said

Countering phishing "stage magic"

Forum members stage monthly phishing attack tests, regularly construct more sophisticated tests, deploy carrot and stick incentives to help employees avoid being exploited and try to strike the right balance in raising the level of employee awareness.

Those actions make sense, given that threat actors are getting increasingly sophisticated in their phishing attacks. Niche threat actors are selling writing and editing services to help other threat actors improve the efficacy of their phishing campaigns by reducing the mistakes that make them

easier to detect. Social engineering attacks are prevalent, often powered by deepfakes that threat actors produce through the Dark Web. They are using cues to make people more susceptible to stimuli. As one CISO said: “Bad guys are really good at getting users to not notice the signs of a phishing attack.”

Conversation about how to empower employees to avoid becoming phishing victims was robust. One Forum member said their enterprise has constructed a tiered phishing testing framework: basic, more sophisticated and opt-in. At the opt-in level, employees volunteer to be tested on their ability to identify extremely sophisticated attacks.

One CISO takes a personalized approach to training repeat employee victims. “We’ll have a 20- to 30-minute conversation and explain, 'It’s not that you failed a test. We succeeded in making the test difficult. Now let us show you what the threat actors are doing so you can look for the signs next time.'”

Another CISO said they have progressive levels of testing and punitive actions aimed at educating repeat offenders. “At some point, they may get internet access restricted or have a bonus reduced. You’ve got to draw the line somewhere.”

Leading practices

- **Look for no/low-cost process improvements**. One CISO found a review of service desk operations uncovered significant opportunities to improve controls. “We’ve seen an increase in the number of phishing calls,” said a CISO. “Tightening up identity identification at the service desk cost basically zero dollars and everybody, including the board, loved it.”
- **Keep training on security practices current**. Social engineering threats, for example, are constantly evolving. Focus on changing user behavior.
- **Be specific about the business impact of bad practices.** Get on senior management’s agenda to explain how attacks can specifically disrupt their business operations.
- **Use multiple vendors to increase protection.** Several Forum members talked about the need for layered controls. Use multiple tools and services to scan external systems/apps since each tool will have different capabilities in identifying vulnerabilities.
- **Eliminate standard passwords.** Access control is critical to greater security. MFA devices need to be checked on a regular basis to ensure no one has registered a rogue device. New employees should be given a unique password for first-time log-in.
- **Tighten privileged access management practices.** Having separate systems and establishing time limits for access can make lateral access much more difficult for threat actors.
- **Prioritize patching external-facing assets,** including devices, appliances and applications— not just for the operating system. Identify and protect the crown jewels of data.
- **Don’t ignore assets on your exception list.** “There may be good reasons why you have an exception list, but threat actors don’t care about those distinctions. They’ll look for vulnerabilities everywhere,” said a subject-matter expert.

- **Keep DevApp teams informed of patching activity.** A common complaint is that the security team finds all the problems but doesn't bring help to fix them**.** Have regular calls with the infrastructure and development teams to help them prioritize issues. One CISO is sponsoring a program that helps DevApp teams patch their applications in advance of a corporate vulnerability directive.
- **Leverage CISA threat intelligence.** For more on this**:** https://www.cisa.gov/cyber-hygiene-services.
- **Minimize expectations about trust with third parties.** While IT partners generally take security seriously, threat actors continue having success with lateral attacks on supply chain partners. "Side-channel attacks are particularly hard to detect," warned 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 699,000 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.