The Weakest Link

MOST COMPANIES rely on external contractors, partners, and suppliers to get business done. As these business partnerships evolve, it’s not uncommon for systems and processes on both sides to be integrated together. We’ve observed that in many cases, the security practices of third parties are overlooked when this sort of integration takes place.

There are many reasons for this. Requiring partners to tighten their security practices, if at all possible, slows business down. Teams and individuals tasked with arranging business partnerships often aren’t security-minded. And when IT departments start integrating systems, they are often pressured to “just get things done”, and end up having to cut corners.

Every third party you work with has the potential to increase your attack surface. This can lead to opportunistic attacks (your partner gets breached and the attacker finds a way into your own systems) or targeted attacks (the attacker researches companies you’re partnered with and finds a way into your network via one of their systems). Any breach that involves an attacker pivoting into your network via a third party can be defined as an upstream attack.

Exposure points in your attack surface can wildly vary based on the type of third party you’re doing business with. There’s a lot of room for creativity when it comes to upstream attacks, and it’s extremely difficult to cover every possible scenario. Here we present you with a few examples of upstream attack vectors that we saw in the field last year.

Facilities services
Companies that provide on-site facilities services, such as garbage collection, cleaning, physical security, and maintenance, get physical access to their customers’ premises as part of their work. This access can include ID badges, keycards, door codes, and maps of the buildings.

We’re all familiar with the fact that, more often than not, cyber attacks originate from different geographic locations than the target they’re attacking. However, when considering methodically planned, targeted attacks, adversaries looking to infiltrate an organization may be willing to go as far as to gain physical access to their target’s premises. In such cases, the attacker may turn to facilities service providers to obtain that access. Indeed, the act of obtaining physical access to an office as part of a targeted attack is something our incident response teams saw happening in Europe during 2016.

Facilities services companies are often quite low-tech. For instance, it’s not uncommon for them to keep...
relevant documents on an open-access file share that workers access to download and print instructions before they leave on assignment. The insecure methodologies employed by-and-large by facilities service providers are ripe for the picking, should an adversary choose to make a physical breach part of their attack.

Our CSS consultants are ever weary of upstream attacks, targeting a primary target via a third-party, and they know from their own red teaming gigs that tactics such as imitating a carpet cleaning company will gain them access to many physical locations.

Information relevant to gaining physical access to offices or homes can also be of value to criminals. The likely geographic proximity of the attacker may lead one to believe that such an attack couldn’t be relevant. But consider this example. A hacker in New York gains the ability to remotely open internet-connected smart locks. However, the locks he gains access to are installed on doors in Europe. It makes no sense for the hacker to travel to Europe and break into those houses, so he puts the information up for sale on the Internet (at let’s say 50 EUR per lock). Local criminals then purchase those lock codes and use them to perform burglaries.

Network-borne attack vectors are enabled when facilities providers are given the ability and access to remotely manage a customer’s infrastructure. The software for managing and controlling alarm systems, cameras, heating systems, and physical access controls is often very old, and written without security in mind. It’s not uncommon for such systems to be accessed over Telnet or VNC, and sometimes with no authentication. You can find plenty of this stuff with Shodan.

In a now classic example of an upstream attack involving a facilities provider, Target was breached in 2013 via a system designed to monitor and control air conditioning hardware. The machine in question was accessible from the Internet and had connectivity with Target’s retail operations. Attackers easily owned the air conditioning monitor. From there, they were able to pivot onto Target’s network, and then onto Target’s point-of-sales systems.

Agencies

Third-party agencies that provide marketing, branding, web presence, recruitment, and eCommerce services are another common ingress point for upstream attacks. These companies often host services which are, in most cases, directly interfaced to their customer’s corporate network. Gaining access to an agency’s systems can provide an attacker with an easy pivot into their customer’s networks.

Consider a web server that hosts sites for multiple companies. Some of these companies will have machines in their corporate network directly interfaced with that web server. If the web server is directly attacked, each individual website it connects to can be attacked (via misconfigurations or
vulnerable plugins). And finally, any of the customers’ networks can be breached, giving an attacker access to the web server and, from there, all of the other interfaced systems. These types of systems have large attack surfaces and are tempting targets for potential adversaries.

Recruitment agencies are also at high risk due to the type of content they deal with on a daily basis. Recruitment agencies deal with job applications, in the form of PDFs and Microsoft Word documents, which constantly arrive from unsolicited sources. These document types are extremely common infection vectors.

Furthermore, recruitment agencies often run their own applicant database systems that are in-sourced by customers. A recruiter receiving a malicious CV might unknowingly upload it to their system, where it is then accessed by dozens of customers (from within their own company networks). All the attacker needs to do is bypass any security or AV product the recruitment agency is using in order to spread the malicious document further.

Malicious documents are not the only attack vector in this scenario. “Applicants” may also link to watering holes from within their CVs or cover letters. In a real-world example from late 2016, our Threat Intelligence team observed several HR departments being targeted by phishing attacks as part of opportunistically targeted ransomware campaigns against businesses.

It goes without saying that the recruitment process is fraught with danger from both spear phishing threats and crimeware.

**Consultants**

Many companies source external staff, in the form of contractors and consultants. Companies that provide consulting and outsourcing services invariably maintain their own security policies (regarding endpoint protection, hardening, document handling, and security awareness guidelines), which are guaranteed to differ from the policies defined by their client companies.

Several high-profile cases over the last few years have illustrated the fact that employees of external services can pose a credible insider risk to an organization.

Consultants receive limited or full access to corporate networks and resources, often via workstations or laptops that often haven’t been issued and configured by the organization they are consulting for. Many companies bring in consultants to set up or maintain financial systems. Software engineers are also commonly outsourced, and these consultants gain access to part, or all, of their customer’s source repositories and version control systems. It’s almost impossible to carefully monitor a consultant’s every move.

When looking for an ingress point during a targeted attack, threat actors sometimes turn to the owners of botnets to rent specific compromised machines that
The Weakest Link

are known to be part of the targeted organization. External contractors widen the net when it comes to finding these already compromised systems. They also widen the net for spear phishing and social engineering attacks.

If your organization routinely uses contractors and external personnel, your physical premises could be more open to social engineering tactics. With so many different faces coming and going on a daily basis, it’s easier to fool employees, and an attacker posing as a consultant might readily be given access to the building, and possibly even secure areas within it. Our CSS consultants use such tactics to great effect when performing threat assessments for customers.

Final advice

When working with third parties, there are a few things you can do to minimize the risk of upstream attacks. Always be cautious when allowing any external device to access your network. Limit access as much as possible. Use tight access controls. If possible, make sure external devices are connected to segregated, controlled networks. Assume the device in question is compromised, and treat it as such.

When bringing in a partner, assess their security practices and, if possible, work with them on improving areas where they’re lacking. At the very least, ask partners to follow a defined set of basic policies and practices. Where possible, audit their systems yourself.

When it comes to on-site staff, provide them with equipment that you’ve set up and configured yourself. Allow them to access only the systems they need to work with, and remove access as soon as they’re finished with the assignment. Make sure you’re able to log their access and the changes they make, and remember to audit those logs.

Be especially aware of legacy systems such as those used to control machinery or infrastructure. If possible, keep these systems isolated and don’t give them access to your corporate network. If you’re giving third parties access to these sort of systems, make sure there are proper authentication and audit mechanisms in place, and that they aren’t open to the Internet.

Keep an eye on what is connecting to your corporate network and what it’s trying to access. This is especially important if you have a lot of external parties coming and going. Run frequent discovery scans on your network, identify unknown systems and services, and shut them down if you find them.

And finally, it’s always good to teach your employees to be aware of social engineering practices in the workplace. Teach them with stories and anecdotes. Have them watch the 1992 film Sneakers, or the recently aired TV show Mr. Robot. Learning about this stuff is fun, and it will engage your staff.

***

“HAVE YOUR EMPLOYEES WATCH THE 1992 FILM SNEAKERS, OR THE RECENTLY AIRED TV SHOW MR. ROBOT”
WE SEE THINGS OTHERS DON’T