The Reality Of IP Theft

Joel Hans, Managing Editor, Manufacturing.net

Verizon has recently released its fifth annual Data Breach Investigations Report (BDIR), which investigates the various ways that attackers — both internal to a company or external, both intentional and accidental — breach security systems and gain access to sensitive data. This year, Verizon's RISK team decided to take a closer look at the data in the effort to discover trends in attacks related directly to intellectual property (IP).

Their findings upturn a number of common misconceptions about IP theft and give credence to new, re-envisioned methods for keeping data safe. Among the most compelling findings are the prevalence of insider agents, along with a heavily increased use of various "social" attacks on employees, which lead them to divulge credentials — or the IP itself — based on personally-crafted trickery.

> Marc Spitler, Senior Risk Analyst,Verizon RISK team

Marc Spitler, a Senior Risk Analyst with Verizon's RISK team, says, "We saw more diversity as far as tactics used by adversaries in these incidents. It is really dominated by malware and hacking. But we've also started to see these other action categories, such as social engineering, pretexting, phishing, as well as misuse."

Who

Based on DBIR data, smaller companies are generally less susceptible to IP-based attacks. Companies with 101 to 1,000 employees suffered an average of 11 breaches, while companies with 1,001 to 10,000 dealt with triple that amount. As the report says, larger companies typically have IP that is more well-known and valuable, making them ideal targets. For major corporations (more than 100,000 employees), however, breaches begin to trail off. The report says that these major firms "typically have more resources to commit to a stronger security posture, so stealing their prized possessions often requires a different strategy."

Mark Spitler, Senior Risk Analyst, Verizon RISK TeamSpitler was keen to point out the relationship between external and internal agents. "Whether working alone or in collusion with external agents, almost half of [IP breaches] have some sort of insider agent directly contributing to the incident," he says. So while a whopping 87 percent of IP breaches involve an agent from outside the company, a large number of those attacks also involve a company employee, malicious or not.

The data shows that 46 percent of breaches were caused by internal agents. Spitler says it's important to remember that by "internal," the report refers to employees who either abuse credentials or unintentionally expose information to the public.

Clicking on a phishing link is counted as an “external” breach. In this light, the prevalence of internal attacks is disconcerting.

How

In order to better make sense of how these IP breaches occur, it’s important to break them apart between external and internal agents.

External

An external breach is any conducted by a party outside of the organization, which includes hackers, or even employees with competitors. Spitler says that “manufacturers would typically not be as likely to be part of those industrialized, scalable attacks” that often afflict retail or financial services companies, such as brute-force hacking. Instead, attackers are using social tactics, such as phishing, to gain access to employee devices with access to secure information.

As seen in Figure 2, 47 percent of all IP breaches involve hacking at some level, which involves the agent using various means to access corporate databases or intranet services through exploits or brute-force attacks. An additional 41 percent involve social angles, which Spitler says is quickly becoming the new normal. These often aren’t “smash-and-grab” efforts, Spitler adds.

Today, more employees are being targeted by spearphishing, which is a targeted attack that is made credible through a certain degree of reconnaissance. This is particularly true for manufacturing. Employees are more likely to click on a link that looks like something they would see on a regular basis. Once gaining access to an individual’s device, attackers often install keyloggers or steal credentials that give them deeper access into the company’s systems.

Internal

When speaking about internal breaches, the report highlighted just how common internal breaches are, and offered some new information as to how and why they occur. 51 percent of all IP breaches can be tied to misuse, which Spitler classified as “indicative of employees that are misusing their access — whether physical or logical — to data.” This doesn’t necessarily have to be malicious, but it often is.

More likely, an employee engages in an insecure workaround to established security measures. Spitler says this is often due to an employee who wants to finish up some work at home. In order to get around a corporate firewall, for example, they copy IP to a flash drive and bring it home, where it is significantly less secure.

But Spitler says that when an internal asset is involved — which accounts for 46 percent of all breaches — it is most likely an intentional, malicious act. 45 percent of breaches involve an abuse of system access or privileges, and 28 percent involve embezzlement or other types of fraud. In addition, a notable portion of internal

attacks come from a terminated employee, whose credentials and access to secure systems was not revoked as part of their termination process.

What

This kind of talk often leaves companies wondering over what more they could be doing to prevent IP thefts, because the truth is that once IP has been accessed, the battle has already been lost.

Spitler says that many manufacturers are “a bit of a step behind” when it comes to IP security. He says that the most important move that a company can make is to step back and get “a good understanding of what is going to be targeted within your environment.” This involves knowing where (physically and logically) IP is stored, and how it is accessed. It’s also important to assess how damaging an IP theft would be to the company.

He adds that one of the most important changes that companies could implement is better monitoring of privileged access. By giving no more privilege than is absolutely necessary prevents employees from being compelled or tricked into handing over valuable information. And the report says, “Privileged use should be logged and generate messages to management. Unplanned, privileged use should generate alarms and be investigated.”

Alerts and logging are mentioned multiple times within the report as critical to the fast response to an IP breach, because breaches are often incredibly quick, while response times are brutally slow. The report shows that 54 percent of attacks are successful within hours, while it most often takes weeks or months for companies to discover that it has been breached. An incredible 31 percent of IP attacks take years to discover. Even after discovery, 53 percent of cases required months to fix, which means that the company is often vulnerable for months, if not multiple years, after the first attack.

The most important takeaway from the Verizon report is, undoubtedly, that IP attacks continue to be prevalent, and that the avenues of breach are numerous. While manufacturers can’t prevent every employee from clicking on a phishing link, or close every gap in their external firewalls, they can implement better security awareness, so that they are left in the dark when attacks occur. As employees continue to bring more devices into the workspace, and as more of our lives — both personal and business — move onto the Internet, these attacks won’t be getting any lighter or less commonplace.

To learn more about the data, and to see the rest of the results for yourself, check out the report *[1].*

Links:
[1] http://www.verizon.com/enterprise/2012dbir/us