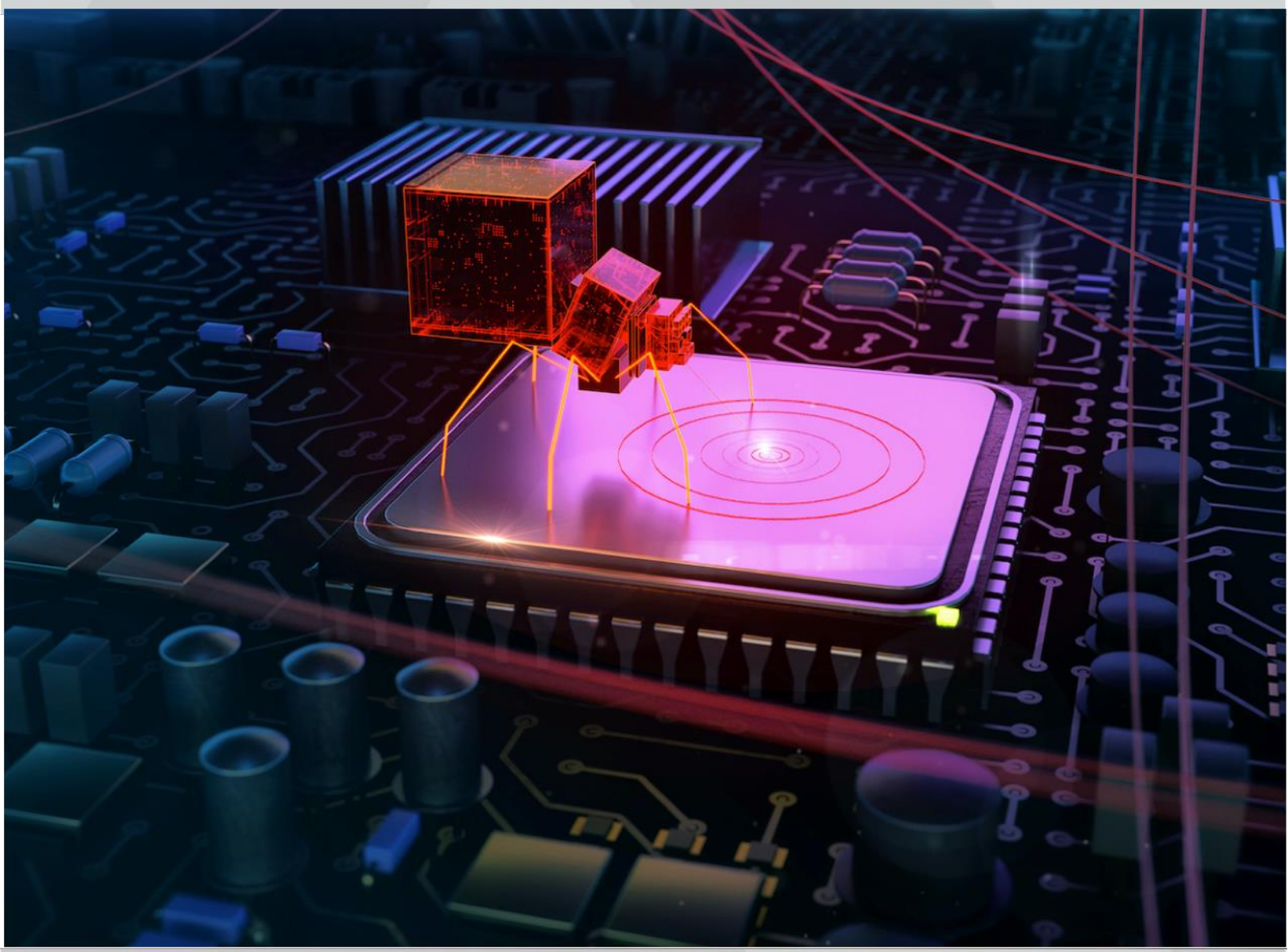
ACTIONABLE INTELLIGENCE

HP Warns That Third-Party Chips Pose Security Risks



THE PRINTER AND SUPPLIES INDUSTRY'S LEADER FOR NEWS AND ANALYSIS

If you found a USB memory stick in a parking lot, you wouldn't take it home and pop it in your home computer, would you? After all, you wouldn't know where the USB stick originated, where it had been, and whether it might contain malware. HP is urging HP printer owners to think the same way about third-party ink and toner cartridges that feature third-party chips.

"A system is only as strong as its weakest link. We see third-party supplies with non-HP chips as a weak link entry point for malicious hackers."

The analogy is how Shivaun Albright, chief technologist for print security for HP Inc., described the potential risk of using third-party cartridges with non-HP chips in HP printers. When printer owners use third-party cartridges with non-HP chips, she warns, "You are putting something in your device that you don't know the provenance of."

Andy Binder, vice president and general manager of office supplies solutions for HP Inc., says, "A system is only as strong as its weakest link. We see third-party supplies with non-HP chips as a weak link entry point for malicious hackers."

Actionable Intelligence spoke with Ms. Albright and Mr. Binder as a follow-up to the news that HP had expanded its Bug Bounty program to include cartridges (see "HP Expands Bug Bounty Program to Focus on Cartridges"). The two discussed how HP works to make its printers and cartridges the most secure in the industry and how third-party cartridges with non-HP chips can compromise that system.

HP Printer Security

Ms. Albright says printing security requires an end-to-end, layered defense strategy. She describes how HP employs overlapping layers of security—for the device and supplies, data, and documents. The next layer is HP's fleet security monitoring, compliance, and management. On top of that is HP's security advisors and services. She describes all the layers as an ecosystem—one that provides HP with differentiation from the competition. All these layers help HP create what Ms. Albright terms "cyber resilient devices," or ones that focus on protecting, detecting, and then recovering.

HP has long focused on print security, but we saw the firm commence a major effort to beef up security, make security a real competitive differentiator, and earn a reputation as offering the most secure printers in the industry in 2015 when HP launched a spate of new technologies including HP Sure Start and self-healing capabilities, whitelisting, and run-time

Under the Bug Bounty program, HP works with Bugcrowd to pay white-hat hackers up to $10,000 to expose weaknesses in HP's security so that the company can address issues before they are exploited by malicious hackers.

intrusion detection in the LaserJet 500 series (see "HP Makes Security the Focus with JetIntelligence-Based LaserJet 500 Series"). These are part of the device/supplies layer in the ecosystem shown in the slide below.

From there, more security improvements followed, as did clever marketing campaigns aimed at increasing end-user awareness of the risks posed by unsecured printers (see "HP Studios' 'Wolf' Stalks Vulnerable Printers"). In 2017, HP assembled an "A team" of cyber security experts to help protect its customers from hacker threats (see "HP Enlists Cyber Security Experts to Outwit Hackers"). In 2018, HP announced its Bug Bounty program (see "HP's Bug Bounty Program Invites Hackers to Find Printer Security Flaws"). Under the Bug Bounty program, HP works with Bugcrowd, a crowd-sourced cyber security organization, to pay white-hat hackers up to $10,000 to expose weaknesses in HP's security so that the company can address issues before they are exploited by malicious hackers.

HP's penetration testing and Bug Bounty are part of what Ms. Albright terms "security hardening." She explains this is essential because while you can incorporate various security features, if there is one vulnerability a hacker can find easily, they can get access to your device and potentially your network.

The new twist on Bug Bounty that HP announced on October 1, 2020, and that caught the attention of many in the supplies industry was HP's decision to expand the program to look at vulnerabilities associated with cartridges. HP announced that as of October 1 it would be working with four professional ethical hackers from Bugcrowd "to identify vulnerabilities in the interfaces associated with the HP Original print cartridges." The program was slated to run for three months.

Dangers of Reprogrammable Chips

Mr. Binder says that the big problem with many third-party chips is that they are reprogrammable. HP's decision to expand the Bug Bounty program to include cartridges was influenced by what HP is seeing in the aftermarket today, he tells us—namely third-party

HP's decision to expand the Bug Bounty program to include cartridges was influenced by what HP is seeing in the aftermarket today—namely third-party chipmakers' increased use and promotion of reprogrammable designs.

Andy Binder, vice president and general manager of office supplies solutions for HP Inc.

chipmakers' increased use and promotion of reprogrammable designs.

Indeed, certain third-party chipmakers are focusing on the fact that their chips are reprogrammable as a selling point. In 2020, Ninestar and its Apex Microelectronics chipmaking arm promoted the capabilities of their Unismart for Firmware Upgrade (UFU) solution, a cloud-based chip-resetting system that can reset Apex chips remotely (see "Ninestar Promotes Its Unismart for Firmware Upgrade Solutions" and "Ninestar YouTube Presentations Introduce New Products and Reveal Pandemic Strategy"). In another example, Chipjet, Hubei Dinglong's chipmaking subsidiary, recently highlighted its ChipStation solution for resetting chips (see "Chipjet's ChipStation Resets Chips Affected by Firmware Updates").

While convenient for third-party supplies firms that must regularly update chips, reprogrammable chips can pose a big risk to printers and the home and corporate networks on which they reside, according to Mr. Binder and Ms. Albright. An attacker with the right skills, motivation, and resources may be able to uncover and exploit a vulnerability, taking advantage of the electronic data interface between the printer and cartridge chip to launch malicious code, change the printer functionality, and put data at risk. Mr. Binder says it may be the case that the major third-party chipmakers aren't themselves introducing malicious software into reprogrammable chips. However, "Others can take advantage of the chips being reprogrammable." He declares, "Reprogrammable chips are not in the best interest of protecting end users."

Ms. Albright concurs. She says, "Clone cartridge vendors are actually marketing the fact you can modify code [on chips]." She shares the USB-in-a-parking-lot analogy with which we began this article and emphasizes that knowing the provenance of the consumables you put inside your printer is essential. Ms. Albright says that in the security world a growing and important area of focus is supply-chain security.

Take, for example, the recent news from the U.S. Cybersecurity and Infrastructure Security Agency (CISA) that U.S. government agencies, critical infrastructure entities, and private sector organizations have been compromised by an advanced persistent threat (APT) actor beginning in at least March 2020. This suspected Russian cyberattack stemmed from a compromised supply chain on certain SolarWinds Orion products.

HP carefully vets its supply-chain suppliers, Ms. Albright tells us, so it knows the provenance of technology and components up and down its supply chain. Whether that is true for third-party consumables isn't always clear.

For example, when you buy a third-party cartridge on eBay or Amazon, you might

Ms. Albright says that third-party chips use general-purpose processors and it is "easy to get in there and reprogram them."

Mr. Binder asserts that HP has seen real cases of third-party chips with malware that allowed the chip to take over the functionality of the printer.

not necessarily even know who is selling it. As we have documented in years of coverage of industry lawsuits and Amazon takedowns on this website, the seller name used on an online marketplace is not necessarily the name of the firm selling you a cartridge—in fact, it seldom is. End users do not necessarily think of all the stops a third-party chip makes on the route from the manufacturer to the end user—from the chip factory, to a cartridge manufacturer, to an exporter, and then from one distributor to another as a cartridge travels around the world. HP wants to encourage end users to think about all the places where a cartridge has traveled and bear in mind that at any stop along a third-party cartridge's route from chipmaker to end user, the reprogrammable chip may have been compromised.

Ms. Albright says this is not the case with HP chips or cartridges. HP has programs in place to ensure supply-chain security starting with the chips and including boxes and cartridge packaging. Moreover, its chips are not reprogrammable. Ms. Albright says HP uses "security-hardened chips" on its inkjet and toner cartridges that "are tamper resistant." Original HP office cartridge chips use secure smart card technology, commonly found on chip-based credit and debit cards. All original HP office printer cartridges introduced since 2015 use smart card technology for maximum data integrity and resistance to tampering and hacking. Smart card technology ensures that the HP proprietary code written to the chip cannot be altered, reprogrammed, or replaced.

In contrast, it is not that hard to compromise third-party chips because they have been specifically designed to be reprogrammable. Ms. Albright says that third-party chips use general-purpose processors and it is "easy to get in there and reprogram them."

Mr. Binder says, "Even if third-party chipmakers like Apex and Zhono don't have ill intent, others can take advantage along the supply chain." He points out that Ninestar is touting its ability to do upgrades in its reprogrammable chips and is "training the aftermarket to do upgrades remotely."

Mr. Binder asserts that HP has seen real cases of third-party chips with malware that allowed the chip to take over the functionality of the printer. In some instances, the chip wouldn't allow end users to print, but he claims compromised chips "can do more nefarious things" like looking at data. "This is a real problem that has happened in the past," he asserts. "That's why we're testing third-party chips with Bug Bounty to see what can be done." He adds, "We know what has happened in past, but we also know the potential value of hacking into chips."

Ms. Albright explains how hackers might exploit a reprogrammable chip. Essentially, a hacker would be looking to exploit the data exchange between the cartridge and the printer. "If malware is injected, the malware 'phones home,'" she says. Typically what will happen next is the hacker uses the malware to look for other exposed devices and "moves laterally across a network." Other IoT devices may be compromised, and, of course, the printer itself is compromised. Hackers can get access to sensitive information such as stored data and print jobs being processed on the printer. She says it is even possible hackers could put listening devices in cartridges.

The two HP experts point out that hacks can happen in places where you don't expect as well as known avenues of attack. In 2014, for example, Target

HP conducted research in 2019 that showed that 48 percent of IT decisionmakers found it believable that clone cartridges pose a security threat.

was attacked by hackers after network credentials were stolen from a vendor that worked on refrigeration, heating, and air conditioning systems at certain Target stores. Any IoT device can pose a risk. If printers, long criticized as being vulnerable, can pose a risk, so too can their supplies. Mr. Binder says HP conducted research in 2019 that showed that 48 percent of IT decisionmakers found it believable that clone cartridges pose a security threat.

Ms. Albright says that HP has been talking a lot with the ethical hackers on its advisory board about cartridges and they agree that consumables can pose a risk. She says it all comes back to the need to focus on supply-chain security. She says that HP's advisors agree that from a supply-chain security standpoint it is critical that you know the provenance of what you are putting in your device.

According to Mr. Binder, that is why HP hired Bugcrowd and expanded Bug Bounty to include consumables. HP wants to uncover and fix any vulnerabilities in the interface between the cartridge and the printer as well as explore whether a cartridge's chip can be "weaponized" by hackers.

More to Come

As noted above, the Bug Bounty program for supplies was due to run for three months, and Mr. Binder confirms that phase one of the cartridge-facing aspect of the program ended December 31. However, due to the value of continuous penetration testing from industry-leading experts, and in an effort to stay one step-ahead of the bad guys, the Bug Bounty program, he says, will likely continue in 2021 and beyond.

Ms. Albright indicates HP is eager to see how skilled ethical hackers can find vulnerabilities, including attacks on printers via cartridges. This is important and valuable work, she says, that will ultimately help protect HP customers.

Actionable Intelligence is eager to hear more from HP about the results of its cartridge-focused Bug Bounty program. We are curious to see if the firm has examples of the dangers posed by reprogrammable chips it can share.

We are also interested to see whether third-party chipmakers respond to HP's assertions that reprogrammable chips pose a security risk because they could be compromised by unethical hackers.

About Actionable Intelligence

Actionable Intelligence is the leading source for news, analysis, and research on the digital printer and MFP industry and the original and third-party consumables business. Actionable Intelligence provides clients with customized research and consulting, as well as up-to-date news and strategic analysis on Action-Intell.com, the industry's leading destination site visited by tens of thousands of printer and supplies executives worldwide. Global printer OEMs, third-party supplies vendors, distributors, resellers, and a diverse mix of other companies rely on Actionable Intelligence to deliver timely and accurate information about the trends shaping the printer hardware and supplies markets. To learn more about Actionable Intelligence, visit www.action-intell.com.