Is Your Printer The New Trojan Horse?

How Can End Users Defend Themselves and Their Organizations?

Executive Summary

Of all the IT devices commonly found in a corporate office, business, school, government building or even home office, the traditional office printer is generally perceived as benign and non-threatening. However, in the age of increasingly sophisticated cybersecurity attacks, the printer's passive functioning is its central attraction as an attack vector for nefarious actors looking for the weakest link in an organization's IT security defense strategy.

Printers pose critical and underappreciated security challenges for office and, particularly, work-at-home users. Through the seemingly harmless printer, hackers can steal IP addresses, sensitive information and data and gain access to corporate and home networks. Once attackers successfully compromise a printer, they can remain dormant as long as they desire and then move laterally into the network, gaining ever-elevated network privileges to exfiltrate critical data or unleash crippling ransomware. This can occur even under the radar of some of the most advanced firewalls and security incident and event management (SIEM) and security vulnerability scanning assessment tools. In effect, the cybersecurity industry is beginning to recognize the printer as a modern "Trojan horse."

This research paper will outline and size the threat and delve into how HP, the largest printer manufacturer in the world, has implemented a pragmatic, efficient and effective strategy to ward off potential threats.

Scoping And Defining The Threat

Scoping the size of the problem aids in understanding the severity of the current situation.

The financial impact of a security breach continues to be staggering. According to a 2020 study by privacy and information management research firm the Ponemon Institute, the global average cost of a data breach was $3.86 million in 2020, 1.5% lower

than in 2019.[1] Regulatory fines, legal fees, security expenses, public relation expenses and lost revenue all contribute to calculating the impact of a data breach. In addition, it's important to point out that this cost per data breach does not include other critical items like client turnover and potential impacts on stock price, brand value and reputation and customer trust. The study also notes that 52% of all data breaches are malicious and, notably, a company typically requires 280 days on average to identify and contain a data breach.

Driving this trend is the fact that hackers and malevolent actors have become more technologically capable and creative in penetrating enterprise and home networks over the past 20 years. Additionally, the rise of the proverbial "smart home" has led to an explosion in unprotected IoT and smart devices that has only exacerbated the situation.

Even the U.S. Department of Homeland Security has issued warnings to the public about cyber threats as they have worked closely with the National Cybersecurity and Communications Integration Center (NCCIC) to assist with reducing the risk of systemic cybersecurity attacks on federal civilian networks.[2]

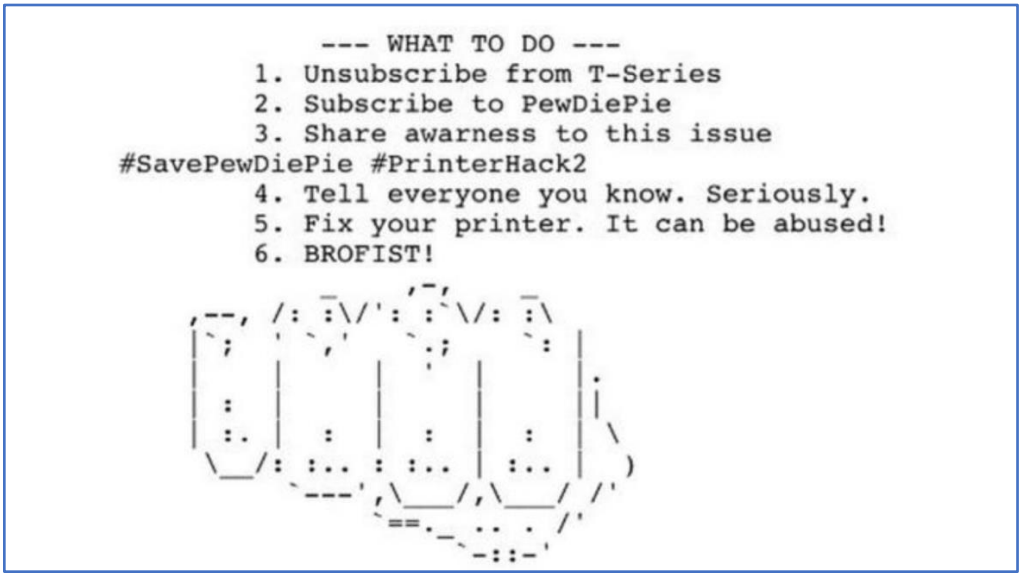
The printer market represents ample opportunity for hackers. Consider that IDC reported 2Q20 printer industry shipments (single-function printers, multifunction printers and single-function digital copiers) of some 20 million units. While much has been made over the past few years about the flatness or even modest decline in the overall printer market, quarterly printer volumes are still substantial. Not only do these multimillion-unit volumes represent an irresistible opportunity for hackers, but this data doesn't include the installed base of more than 2 *billion* units between 2015 and 2019.[3]

Typical printer attacks exploit older versions of firmware, allowing hackers to control and disrupt operations (e.g., losing printing and scanning access for a few minutes or longer). More serious printer attacks may exploit buffer overflows (injection attacks), sensitive data exposure (man-in-the-middle, or MITM, attacks) and open ports or vulnerable protocols (security misconfiguration attacks). ZDNet recently reported that the IPP ports of 80,000 printers were publicly exposed on the internet without adequate firewall protection.[4]

[1] https://securityintelligence.com/posts/whats-new-2020-cost-of-a-data-breach-report/
[2] https://www.dhs.gov/how-do-i/protect-myself-cyber-attacks
[3] IDC WW Hardcopy Peripherals Tracker; 2020Q2 release
[4] www.zdnet.com/article/80000-printers-are-exposing-their-ipp-port-online/

A well-known attack from 2018, dubbed the “PewDiePie” incident, saw some 50,000 printers worldwide hacked and hijacked, resulting in affected units printing the message below.[5]

FIGURE 1: THE PEWDIEPIE MESSAGE



Source: BBC.com

Whether this hack was a mischievous prank or an egotistical (but frightening) demonstration, it’s convincing evidence that the threat is real and tangible.

SECURE FIRMWARE: AN EFFECTIVE CYBERSECURITY APPROACH FOR PRINTERS

HP, the world’s #1 maker of printers[6], is combating the risk to printer security with an intelligently layered defense-in-depth approach. HP takes an end-to-end security architecture approach, from the design of printers to the design of management and monitoring infrastructure and mechanisms for supplying authenticity verification. It also emphasizes secure development and risk mitigation in the supply chain to protect product integrity. HP’s printer security architecture design starts from the hardware, which includes layers of protection to help detect and remediate successful attacks. HP Enterprise and HP Managed LaserJet and PageWide products running FutureSmart

[5] https://www.bbc.com/news/technology-46552339
[6] https://www.statista.com/statistics/541347/worldwide-printer-market-vendor-shares/

firmware have the industry's strongest security; key technologies such as Sure Start and Runtime Intrusion Detection that are always on guard, detecting and stopping threats while adapting to new ones. The potential payoffs for enterprise and SMB users are substantial and durable and include:

- Avoidance of identity and data theft
- Protection, detection and recovery from malware attacks to help secure the broader IT network
- Mitigation of confidential information breaches that can minimize revenue and pose huge financial consequences

CONSUMABLES

Consumables may not be top-of-mind when considering the security vulnerabilities of printers; however, attacks on printers via compromised consumables are not without precedent. Samsung was victimized in 2013 when compromised toner cartridges changed printer settings on Samsung printers allowing them to only use the attacker's brand of cartridges.[7]

In 2015 HP began using secure microcontrollers incorporating firmware with integrated security in original HP inkjet and toner cartridges for all HP Office-class printing systems.[8] According to data that was shared with Moor Insights & Strategy during an interview with HP, a majority of its office printer shipments fall in this category.[9] It should be noted that using non-HP cartridges with non-HP chips with HP printers may cause a security risk.

The firmware included on HP cartridges facilitates the essential operation of the printer. Designed to be protected and impervious to altering, HP's proprietary cartridge chip firmware uses a secure microcontroller attached to the ink or toner cartridge. From a customer experience standpoint, the embedded firmware approach offers tangible advantages. It is seamless and worry-free as customers are encouraged to download the latest firmware to protect their printer from outside attacks. Additionally, authorized

[7] https://www.therecycler.com/posts/virus-alert-for-samsung-cartridge-chips/
[8] HP office-class printing systems are select Enterprise and Managed devices with FutureSmart firmware 4.5 and up, Pro devices, LaserJet models 200 and up, with respective Original HP Toner, PageWide and Ink Cartridges. Does not include HP integrated printhead cartridges. Digital supply-chain tracking, hardware & packaging security features vary locally by SKU. See www.hp.com/go/SuppliesThatProtect and hp.com/go/SuppliesSecurityClaims)
[9] Interview with HP (7-23-20)

HP firmware is crucial as reprogrammable imitation cartridges may incorporate chips of questionable origin utilizing untrusted firmware.

Since 2015 HP chips use custom secure smart card technology, commonly found on chip-based credit and debit cards.[10] By utilizing this technology, HP achieves maximum data integrity with the best-known resistance to hacking and altering. This technique effectively eliminates the security risk that imitation supplies cause as the print cartridge plays such a critical role in protecting the overall print system from cybersecurity attacks.

From a supply chain standpoint, it's also important to point out that HP manufactures chips in secure facilities producing microcontrollers, some of which are explicitly certified as EAL5+. This vital distinction permits HP to gain maximum assurance based on rigorous commercial development best practices.[11]

IT decision-makers recognize the vulnerability of consumables. A 2019 study by HP showed that 48% of surveyed customers find it believable that an unsecured, reprogrammable print cartridge can pose a security threat. Therefore, the types of protection HP provides enables a substantially higher level of confidence that potential "backdoors" haven't been surreptitiously injected into the cartridge's firmware, putting HP printers at risk.

Despite this welcome focus on security, the cynic might ask if the "Original HP" consumables program is merely a shallow marketing ploy to require its customers to pay a premium for HP supplies. It's a reasonable question to ask, given that the rise of smartphones and other mobile devices has helped shrink the printer market by substantially reducing the need to print. This security issue, however, is an industrywide phenomenon that has impacted every printer manufacturer over the past decade. And the fact remains that HP printers using non-HP cartridges with non-HP chips may be a security risk.

HP also claims it has shifted its strategy over the past several years to make printing more affordable and convenient. For example, HP has tried to economize the cost of print with its "Instant Ink" initiative, which is essentially a group of subscription programs (based on anticipated print volumes) that allows consumers and businesses to save up to 50% on ink by letting their HP printer automatically and proactively order home-delivered ink cartridges. The company introduced this program in 2013. More recently,

[10] https://www.thalesgroup.com/en/markets/digital-identity-and-security/technology/smart-cards-basics
[11] https://us-cert.cisa.gov/bsi/articles/best-practices/requirements-engineering/the-common-criteria

HP has announced Neverstop monochrome laser printers that utilize replacement kits of toner, which facilitates a typical sub-one cent cost per page with 5,000 pages of toner included. These actions demonstrate that HP has been working to take cost off the table as a reason for users not to buy genuine HP supplies.

FIGURE 2: FIRMWARE LOCATION ON HP TONER CARTRIDGE

Source: HP, Inc.

THE PRINTER

Conventional security techniques that focus on preventing intrusions at the client PC, workstation, firewall or router levels are often insufficient for thoroughly protecting printers. HP's security implementation gave rise to a "world's most secure printers"[12] strategy based on multiple capabilities.[13]

[12] HP's most advanced embedded security features are available on HP Enterprise and HP Managed devices with HP FutureSmart firmware 4.5 or above. Claim based on HP review of 2019 published features of competitive in-class printers. Only HP offers a combination of security features to automatically detect, stop, and recover from attacks with a self-healing reboot, in alignment with NIST SP 800-193 guidelines for device cyber resiliency. For more information, visit: www.hp.com/go/PrinterSecurityClaims.) HP Enterprise & Managed LaserJets and PageWide.
[13] HP Sure Start BIOS protection, Run-time Intrusion Detection & HP Connection Inspector all with self-

Customers expect manufacturers to provide the latest firmware versions and fixes for security vulnerabilities. HP delivers ongoing firmware security enhancements with "Secure by Default" device security improvements that continually increase device resiliency.

Security experts regard HP's firmware-based approach as the most fundamentally effective way to create highly secure endpoint devices.[14] Like a PC, printers include a firmware-based BIOS, which is a set of boot instructions used to load essential hardware components during the boot-up phase.

The embedded firmware found in HP consumables complements other security protection protocols available in the printer. HP's secure firmware approach at the printer level provides IT managers with numerous benefits from a protect, detect and recover standpoint. HP Sure Start technology, which is the company's brand name for its secure PC-level firmware protection at the BIOS level, works behind the scenes to validate the integrity of the BIOS during power-up. HP Enterprise-class printers utilize company-developed firmware, dubbed FutureSmart, to provide integrity checking down to the BIOS level. If the BIOS is determined to be compromised, the device restarts using a safe "golden copy" of its BIOS without IT intervention. HP firmware is code-signed and validated and Common Criteria Certified, with the most advanced whitelisting techniques and a proven way to prevent attacks on the printer and network.

The first, best step to optimize the security of your printer fleet is to frequently update device firmware to ensure you are running the latest security patches and functional improvements. Many of HP's cloud-connected Consumer and Pro printers have the ability for automatic firmware updates to ensure customers are running the latest and most secure versions. Enterprises with larger fleets of printers generally prefer to schedule their firmware updates at opportune operational times to ensure minimal disruption. Regardless, "Think Firmware First" is a best security practice mantra for anyone with a printer and a proven way to increase your print network's long-term security posture.

healing: the only embedded device capabilities that monitor for threats in real-time including both inbound device write-protected memory (Run-time Intrusion Detection with self-healing, now Common Criteria Certified) and outbound network behavior anomaly detection (HP Connection Inspector with self-healing) in addition to hardware-based HP Sure Start BIOS protection that all automatically recover from attacks by initiating a self-healing device reboot and recovery to secure run-time state without requiring IT or admin intervention.

[14] http://solidsystemsllc.com/firmware-security/

Even product packaging has played a role in HP's single-minded focus on printer security, especially in the consumables realm. HP produces cartridges with specialized construction designs and adhesives that make their packaging virtually tamper-resistant. In some cases, the print cartridge itself is sealed in a zip-strip inner package with a tamper-evident label on a tear strip for further protection.[15]

Implications and Conclusions

From an industrywide perspective, it is hard to dismiss the "Trojan horse" nature of cybersecurity risks posed by the network-connected printer. The sheer number of potentially exposed printers, both from installed base and new shipments, as well as the number of consumables used each year, represent opportunity for hackers and cybercriminals. Compounding the danger of this situation is that the seriousness of the problem is only now getting the attention it deserves, particularly among IT and security professionals.

While other techniques (security software, VPN, router-level security, etc.) have long existed to protect client PC and even mobile devices, the network-enabled printer is often ignored as a potential vulnerability point. As a result, printer configuration settings that result in unused ports or exposed protocols can be an open door for any random or targeted attack.

As a longtime leader across virtually every segment of the printer market in which it participates, HP has a responsibility to provide genuine market leadership. The company has been a leader in print security since 2015, establishing new industry cybersecurity standards and garnering praise from third-party security testing labs for having the most secure printers. HP launched the industry's first Print Security Bug Bounty Program to pay white hat researchers up to $10,000 per vulnerability found in HP Enterprise printers during product development.[16]

For a half-decade, it has mitigated the risk of printer-based network attacks through its secure firmware program at the consumables and device level. HP has always been a brand associated with innovation, and it is satisfying to see the 81-year old company extend that affinity for continuous improvement to all aspects of design and development with security as a primary focus.

[15] Packaging security features vary locally by SKU.
[16] https://press.hp.com/us/en/press-releases/2018/hp-launches-industrys-first-print-security-bug-bounty-program.html)

However, despite all this progress in enhancing printer security, HP must do more. HP should extend this essential embedded firmware capability to all its printers, particularly its low-end consumer-class printers. COVID-19's impact has forced unprecedented numbers of employees to work from home, many using personally-owned pre-2015 consumer-class printers. These workers require robust cybersecurity protection too, and businesses that place company-owned printers in remote work-at-home environments want to manage those printers remotely and ensure their security compliance.

Finally, HP must leverage its vaunted omnichannel approach, which sells the vast majority of both HP's printers and consumables to enterprise and SMB accounts, to underscore the cybersecurity risk message. Recent HP focus group research indicates that IT managers, when properly educated, understand the threat and want to respond appropriately.[17] IT managers will appreciate the communication as HP's printer competitors are not robustly talking about this topic. With the cost of consumables becoming less of an issue for many IT managers, HP should be providing compelling educational materials to drive enhanced awareness. After all, HP is a trusted brand – a leader in quality, reliability and sustainability – that can now expand its printer security leadership.

Although the printer market has been challenging over the past 10 years amid changes in printing behavior, the company has a remarkable opportunity to solidify and extend its position. With the right educational efforts tailored to its channel partners, HP's ongoing work in this area should benefit the overall market. Even after COVID-19 subsides, many work-from-home users are unlikely to return to their offices. These users, who may not enjoy the security protocols provided to them by working in a traditional office, will need as much protection as possible. HP's leadership in this area, particularly as it expands its secure hardware features and firmware approach to all its imaging devices, could not come at a better time.

[17] Interview with HP (7-28-20)

IMPORTANT INFORMATION ABOUT THIS PAPER

CONTRIBUTOR
Mark Vena, Senior Analyst at Moor Insights & Strategy

PUBLISHER
Patrick Moorhead, Founder, President, & Principal Analyst at Moor Insights & Strategy

INQUIRIES
Contact us if you would like to discuss this report, and Moor Insights & Strategy will respond promptly.

CITATIONS
This paper can be cited by accredited press and analysts but must be cited in-context, displaying author's name, author's title, and "Moor Insights & Strategy". Non-press and non-analysts must receive prior written permission by Moor Insights & Strategy for any citations.

LICENSING

DISCLOSURES
This paper was commissioned by HP Inc. Moor Insights & Strategy provides research, analysis, advising, and consulting to many high-tech companies mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

DISCLAIMER
The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Moor Insights & Strategy disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of Moor Insights & Strategy and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

Moor Insights & Strategy provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.