SCREWED DRIVERS OPEN ATMS TO ATTACK

Windows Drivers Used in ATM, POS and Other Devices Allow Arbitrary Access to I/O Ports, Allow Attackers to Target Data to and from PCI-connected Devices

Over the past year, we have repeatedly dug into the problem of insecure and malicious drivers and the risks they pose to Windows-based systems. You can find our previous research here and here. At its highest level, the problem behind "screwed drivers" boils down to two important issues:

1. Vulnerable or poorly designed drivers (often created by technology vendors for managing or updating their products) can be used by attackers to gain control over the Windows kernel and underlying device firmware. As an example, malware has abused these drivers to implant backdoors in victim devices, allowing the threat to persist even after the device is reimaged.

2. There is not a universally applicable way to prevent Windows from loading bad drivers once they've been identified. Microsoft's HVCI technology may protect newer devices, but devices on anything but the latest hardware must rely on manually updated blacklists. Of note, Microsoft has published Windows Defender updates to block vulnerable drivers for the few vendors who specifically requested that their older drivers be blocked.

In previous publications we emphasized that the identified vulnerability is based on a method that is widely integrated in driver software used by the computer industry.

Our latest update to this line of research looks at how the problem of poorly designed drivers applies to devices in highly regulated environments such as ATMs and point-of-sale (POS) devices, and some of the unique challenges they pose.

THE RISE OF ATM ATTACKS

ATMs have long been a target for criminals, and many traditional attacks focused on physically breaking into the cash safes where money is stored within the ATM. However, over the past decade, criminals have progressed to logic-based attacks that trick machines into dispensing cash. Also known as "jackpotting", these attacks can involve malware, network-based attacks, or directly attaching hacking tools to various components of the ATM.

The first ATM malware arrived in 2009 with the discovery of the "Skimer" malware and attack group. As the name implies, this malware focused on capturing information from the card reader and PIN pad of the ATM to steal card information. ATM attacks quickly evolved with the introduction of a variety of new techniques and strategies. The Tyupkin malware discovered in 2014 introduced jackpotting attacks where the malware instructed cash cassettes within the ATM to dispense money. Jackpotting became a staple of ATM-based attacks, and the ATM malware landscape evolved quickly in the following years, with ATM-based malware attacks more than doubling between 2017 and 2019. Some of the more notable

malware variants included WinPot, ATMTest, ATMDtruck, Metel Malware, ATMJackpot, Ploutus, ATMWizX and XFS_DIRECT.

Attacks against ATMs can also take a variety of forms. Attackers can deliver malware by compromising the banking network connected to the device, by compromising the device's connection to card processors, or by gaining access to the ATM's internal computer. And much like traditional attacks, attackers or malware often need to escalate privileges on the victim device to gain deeper access into the system. This is where the use of malicious or vulnerable drivers comes into play. By taking advantage of the functionality in insecure drivers, attacks or their malware can gain new privileges, access information, and ultimately steal money or customer data.

EXAMPLE OF A VULNERABLE DRIVER IN A DIEBOLD NIXDORF ATM

Our recent research into a Diebold Nixdorf ATM provides an example of a vulnerable driver in an ATM. It is important to note that compared to some of the other drivers analyzed in our previous research, the Diebold Nixdorf driver exposes far fewer capabilities, and thus poses a lower risk in the context of an attack. Based on currently available information, the identified vulnerability was not utilized in any known Jackpotting (or other) attack against ATM or POS terminals. However, it illustrates how these same vulnerabilities can exist and be abused in non-standard Windows devices such as ATMs, POS machines and other devices.

Our analysis began by acquiring the internal computer (SWAP-PC 5G i5-4570 AMT TPMen) used in a Diebold Nixdorf ATM. This component can be seen highlighted in red in the image below.

The computer within an ATM naturally plays a central role in the operation of the device. This computer connects to all the various critical components of the ATM such as the card reader, PIN pad, network interfaces, and ultimately, the cash cassettes.

With access to the ATM computer we were able to analyze the drivers available on the device. After inspection we found that a driver was providing arbitrary access to x86 I/O ports on the system. While this is a relatively limited set of functionality compared to other drivers we have analyzed, it is not without its uses. By gaining arbitrary access to the I/O ports, an attacker could potentially gain arbitrary PCI access, which in turn could allow the attacker to target data to and from PCI-connected devices. In addition, this driver is used by Diebold Nixdorf's tool to update BIOS firmware on this device, which indicates that it is a path to modify firmware and could potentially be used to install a persistent bootkit.

While we have not investigated other Diebold Nixdorf models, it is probable that the same driver was used across many of the company's Windows-based ATM and POS products, exposing a broad array of devices to this vulnerability. Diebold Nixdorf responded promptly to our disclosure and worked cooperatively with Eclypsium to understand and mitigate this issue. Software updates to address the vulnerability identified by our research have been implemented and were released earlier this year.

But this is just the tip of the iceberg in terms of what malicious drivers are capable of. Our previous research has identified drivers that in addition to arbitrary I/O access, also had the ability to read/write to memory, Model Specific, debug, and control registers, as well as arbitrary PCI access. These capabilities in a vulnerable driver could have a devastating impact on ATM or POS devices. Given that many of the drivers in these devices have not been closely analyzed, they are likely to contain undiscovered vulnerabilities.

THE SECURITY CATCH-22 OF REGULATED DEVICES

Unfortunately it is not always easy to fix problems in ATMs, POS, and other financial devices when a vulnerable driver is found. First and foremost, these devices are highly regulated. And while strong regulations play an important role in establishing security standards for these devices, they can also inadvertently make updates slower. For example, devices may require a variety of certifications such as Common Criteria, FIPS 140-2, or others. Changes to the device may require the vendor to repeat the certification process, which can take considerable time and effort. As a result, it is not uncommon for vendors to take up to a year or more before delivering an update to a device in a regulated environment. In fact, our research in the Diebold Nixdorf device above was completed in May of 2019, but needed to be held back in order to ensure responsible disclosure and give Diebold Nixdorf the necessary time to make changes.

ATMs and other financial devices can also be an operational challenge to update. Devices are naturally widely distributed, and heavily secured to prevent physical tampering or abuse. Updates to critical drivers may require skilled technicians to physically open and access the device in the field, which can make updating a fleet of devices a particularly long process.

Lastly, many of these devices have long refresh cycles and often rely on older embedded versions of the Windows operating system. A recent analysis of ATMs showed that Windows 7 and Windows XP remain incredibly common with ATMs today. These older operating systems not only increase the potential for vulnerabilities, but also means the devices are unlikely to get OS updates that include driver blacklists. In short, protection will need to come from the vendor-supplied update process described above.

CONCLUSION

Vulnerable and malicious drivers remain a serious issue for a large percentage of Windows-based devices, particularly older devices such as ATM or POS machines. The ability for these vulnerable drivers to gain low-level access to the hardware and information on these systems opens a wealth of potential attack scenarios from jackpotting the device to stealing cardholder data. Furthermore the arduous regulatory and operational work required to update devices can mean that vulnerable devices can remain exposed for long periods of time.