wontok™ SafeCentral SafeDesktop

Malware Prevention for Automated Teller and Banking Machines

Safe, secure transactions for banks and their customers

Financial institutions and their customers are under constant attack from organized crime.

Today, the world's more than 3 million ATMs face many types of attacks — from direct physical assaults such as ramming or removing them from their locations, to skimmers that steal the data encoded on the magnetic or "mag" strips of ATM cards, to more insidious, hidden methods such as malware that can infiltrate internal data networks and steal account information. Since the majority of the world's ATM machines run on Microsoft® Windows®, this means they are as vulnerable to malware as a typical computer. And this threat has become more serious now that Microsoft has ended support of Windows XP. NCR estimates that 95% of the world's ATM machines run Windows XP.

The first ATM malware surfaced in 2007 when a Trojan virus was utilized to attack ATMs in the Ukraine and Russia. Since then, ATM malware has increased and spread across the globe, appearing in the United States in 2010.

Today, the two most common forms of ATM malware are hijacking and excess cash dispensing. Hijacking malware is installed on the ATM and steals a copy of the customer's PIN and card information. Cash dispense in excess malware requires the hacker to rewrite portions of the ATM software and install it on the host. Then a criminal or host goes to the ATM with a trigger card that sends altered code instructions to pass large amounts of currency to the criminal. Most recently, ATMs in Mexico were targeted by a new strain of malware known as Ploutus that allowed criminals to manipulate the denominations of the bills dispensed.

No longer receiving patches and updates, Windows XP-based ATMs will be vulnerable to increasingly sophisticated and frequent malware attacks.

+ ATMs connected to private networks, rather than the internet, are still at risk for infection when malware is deployed over that network.
+ Whether you are running Windows XP, Windows XP Embedded, or Windows 7 Embedded, an additional layer of protection can protect against financial malware, zero day exploits, Trojans and keyloggers that can threaten even Windows XP embedded.

ADDRESS THE RISK OF ATM MALWARE HEAD ON WITH AN ADDED LAYER OF DEFENSE.

If you need to keep your XP system due to system restrictions, budget constraints, or concerns about new risks inherent in hardware upgrades, then you need to look at compensating security controls. Wontok™ SafeCentral ATM should be part of your overall strategy to protect your XP system against threats. Wontok SafeCentral ATM for Windows is different from antivirus or firewalls and can be used in conjunction with your current security solutions. Because it operates deep within the operating system, Wontok SafeCentral effectively creates a barricade against advanced threats and data stealing malware. Wontok SafeCentral is a light-weight software solution that creates a barrier between the ATM application and the Windows operating system. It is cost effective and does not require frequent updates.

Wontok SafeCentral difference

+ SafeCentral fills the gaps left by traditional antivirus, firewalls and encryption technology.
+ SafeCentral locks out man-in-the-middle and man-in-the-browser attacks.
+ SafeCentral defeats advanced malware, including ring zero rootkits.
+ Wontok SafeCentral's Trusted Security Extensions includes kernel drivers and hardened services that supervise operating system's events and enforce policies to block malware and other unauthorized applications on ATMs.
+ SafeCentral integrates seamlessly with other authentication and security solutions.
+ Easy to implement.
+ Supported internationally.
+ SafeCentral ATM is an ideal security measure for devices on closed networks.
+ Patented kernel level security provides secure barrier between Windows and ATM software.

Protects transactions on Windows based ATMs:

+ Prevents ATM hijacking
+ Reduces risk of excess cash disbursement
+ Regulatory compliance
+ Compatible with third party financial platforms
+ Deploys quickly and easily
+ Reduces legal risk
+ Strengthens fraud mitigation strategies
+ Provides security with flexibility
+ Protects your brand and goodwill

Protects against ATM malware threats:

+ Man-in-the-browser, man- in-the-middle and zero-day malware
+ Vulnerability exploitation
+ Keylogging
+ Screen capture
+ DNS compromise and redirection
+ SSL hijacking
+ Password theft
+ Session takeover
+ Registry, process or file tampering
+ Locks out unauthorized applications via USB drives from gaining access to the transactions

Supported systems:

Windows XP, Vista, 7, 8, 8.1, 10 (32 and 64 bit modes), multi-language capability.

Contact Information

San Francisco – USA
americas@wontok.com
+ 1 561 472 5200

Hong Kong
apac@wontok.com
+ 852 2824 8330

Sydney – Australia
anz@wontok.com
+ 61 2 8355 5270

http://linkd.in/1hZrjk1 Twitter: @SafeCentral

www.wontok.com

wontok™