MINERVA

Solution Brief

Malware Protection for ATMs

The success of jackpotting and other malware-enabled attacks on ATMs highlight the challenges of securing ATM devices against motivated adversaries. These devices often use older hardware and operating systems, lack reliable network connectivity for updates, and are difficult to manage due to their distributed locations. As the result, it's impractical to rely solely on technologies such as antivirus and application whitelisting for safeguarding these critical assets. ATM attacks bypass such baseline security controls, allowing criminals to dispense cash and steal customer data. Minerva's Anti-Evasion Platform is effective at protecting ATMs from these threats even when attackers bypass other security measures.

Safeguarding ATM Applications

Cyber-criminals employ specialized malware to interface with ATM software to dispense cash. Minerva's Anti-Evasion Platform prevents malicious code from interacting with ATM middleware components such as XFS. As the result, even if malware finds a way to run on the ATM, it will be unable to direct the ATM application to take unauthorized actions.
Upon preventing the attack, Minerva notifies the IT team about the security event. However, even if the organization is unable to respond to the incident right away, the ATM remains in a protected state, with the attackers failing to reach their objective.

Event Summary

Process Name:	Ripper.exe
File Hash (SHA-256):	cc85e8ca86c787a1c031e67242e23f4ef503840739f9cdc7e18a48e4a6773b38
Certificate Information:	N/A
Rule Category:	ATM Protection 1
Additional Information:	Protected Assest: MSXFS.dll

Minerva prevents malware from directing ATM software to dispense cash without authorization

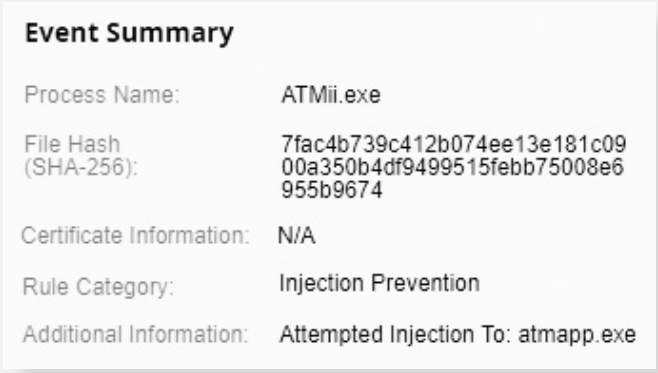
Key Benefits:

- *Protect the critical ATM middleware layer from malware attacks*
- *Continuous protection even when no network connectivity*
- *Supports legacy and newer Windows version via a single agent*
- *Easy to deploy and operate across disconnected and dispersed devices*

Multi-Layered Protection

Minerva's Anti-Evasion Platform provides reliable and comprehensive safeguards against ATM malware. Each component reinforces the others to offer the widest threat coverage against the techniques used to bypass existing defenses. For instance:

- **Prevent a broad spectrum of ATM malware,** such as Ripper, GreenDispenser, and many others to block malicious code from interacting with ATM middleware and thwart unauthorized withdrawals.
- **Stop malicious code from being injected into the memory of ATM applications**, a technique employed by malware such as ATMii.
- **Simulate the tracks malware leaves behind**—the infection markers—to fool malware into refusing to run on the ATM, an approach useful for blocking malware such as Ploutus.
- **Disarm ATM malware** by automatically mimicking security artifacts related to the environment that some ATM malware families, such as Tyupkin, are designed to avoid.



Minerva prevents malware from injecting malicious code into ATM software

```
bool result;
try
{
    Mutex.OpenExisting("DIEBOLDPL");
    return false;
}
catch
{
    Class5.mutex_0 = new Mutex(true, "DIEBOLDPL");
    result = true;
}
return result;
```

Excerpt from malware designed to avoid infecting the ATM if it believes the device is already infected

Built for the Real World

Minerva's ATM security capabilities are built to accommodate the challenges of real-world ATM deployments. Our solution maintains its effectiveness even if the ATM is not connected to the network. Minerva is compatible with all variants of Microsoft Windows, including older OS versions, and can operate even on underpowered systems. Moreover, Minerva doesn't require burdensome configuration or maintenance tasks.

Safeguards ATMs even when AV or app whitelisting fails

Designed for distributed, unattended operations.

Compatible with modern and legacy OS and hardware.

About Minerva

Minerva is an innovative endpoint security solution provider that protects enterprises from today's stealthiest attacks without the need to detect threats first, all before any damage has been done. Minerva Anti-Evasion Platform blocks unknown threats which evade existing defenses by deceiving the malware and controlling how it perceives its environment. Without relying on signatures, models or behavioral patterns, Minerva's solution deceives the malware and causes it to disarm itself, thwarting it before the need to engage costly security resources.
Headquartered in Petach Tikva, Israel, and with offices in New York and Atlanta, Minerva boost customers' existing defenses without the need to embark upon a costly and risky overhaul of their entire endpoint security architecture. To learn more about Minerva, visit **www.minerva-labs.com.**