ENCRYPTION CONSULTING

CASE STUDY

PKI ASSESSMENT & SUPPORT

The 2023 MSI code signing data theft and how CodeSign Secure prevents it

In 2023, a ransomware gang stole MSI's firmware signing and Intel Boot Guard keys and leaked them on the dark web. The keys can't be revoked, and the risk of malicious firmware lingers, a textbook case for hardware-protected signing.

SUBJECT	INCIDENT	FOCUS
MSI (Micro-Star Intl.)	2023 ransomware leak	Firmware signing keys

1.5TB
Sensitive data stolen

116
Intel Boot Guard keys leaked

$4M
Ransom demanded, refused

MSI, a leader in gaming hardware

Founded in 1986 and headquartered in New Taipei City, Micro-Star International (MSI) is a globally recognized Taiwanese technology company and a leader in gaming and professional computing. Its portfolio spans motherboards, graphics cards, laptops, desktops, servers, industrial PCs, and gaming peripherals, with operations across more than 120 countries and thousands of employees.

For a hardware vendor like MSI, firmware signing is a critical security function. It ensures that only legitimate, untampered firmware can run on a device, forming the foundation of a secure boot process. That makes the keys behind it some of the most sensitive assets the company holds.

When signing keys are fused into the hardware itself, protecting them isn't optional. If they leak, there is no easy way to take them back.

A theft that can't be undone

A ransomware attack turned MSI's most sensitive signing keys into public, permanent risk.

1

A ransomware gang struck

In March 2023 the Money Message gang breached MSI, took about 1.5 TB of data including source code and signing keys, and demanded a $4 million ransom.

2

Signing keys leaked

When MSI refused to pay, the gang published the data, including firmware signing keys for 57 products and Intel Boot Guard keys for 116 more.

3

Keys that can't be revoked

Boot Guard keys are fused into the chipset at manufacturing, so they can't be revoked or replaced without changing the hardware, leaving devices exposed.

4

Boot Guard bypassed

With those keys, attackers could sign malicious firmware that slips past Intel Boot Guard, opening the door to rootkits running below the operating system.

5

Weak monitoring, lasting fallout

The breach pointed to gaps in tamper-evident logging and SIEM monitoring for key usage, and it left MSI facing eroded customer trust, costly audits, and regulatory exposure.

> The MSI breach traced back to six gaps: unprotected keys, no access controls, no audit trail, an irrevocable root of trust, an exposed update channel, and no compliance baseline. These are infrastructure problems, and they require infrastructure-level fixes.

ENCRYPTION CONSULTING, CODESIGN SECURE TEAM
CODESIGN SECURE: ENCRYPTION CONSULTING · CODE SIGNING SECURITY

How CodeSign Secure would have stopped it

CodeSign Secure protects signing keys in hardware and controls who can ever use them, so a stolen file is worthless without the key that never left the HSM.

HSM-protected keys

Keys are generated, stored, and used inside FIPS 140-2 Level 3 HSMs from vendors like Thales, Utimaco, and Fortanix, and never leave the device.

Automated signing pipelines

Signing integrates with CI/CD tools like Azure DevOps, Jenkins, and GitLab, including firmware pipelines, enforcing policy and cutting human error.

Granular access controls

Role-based access, multi-factor authentication, and M of N quorum approvals ensure only trusted people can ever initiate a signing operation.

Signed audit trails

Detailed, signed logs and secure timestamps (RFC 3161, Authenticode) give real-time visibility and forensic proof for every signing event.

Post-quantum ready

Support for NIST-approved PQC algorithms like ML-DSA and LMS future-proofs signing against the next generation of cryptographic threats.

Compliance and SBOMs

The platform aligns with FIPS 140-2, CA/ Browser Forum, and GDPR, and integrates vulnerability scanners and SBOMs for supply chain transparency.

04 THE IMPACT

A threat that outlives the breach

No fix can pull the leaked keys back. The danger lives on in the firmware trust chain, which is what makes this breach so serious.

$46B

What's at stake when signing keys leak

BEFORE — keys exposed

AFTER — keys in HSM

Firmware-level malware

Stolen keys can sign malware that hides in UEFI flash below the OS, surviving reinstalls, drive swaps, and even factory resets.

Software supply chain at risk

Trusted firmware channels could carry malware to many organizations, part of a supply chain attack problem estimated at $46 billion globally.

Reputation and revenue

The breach shook customer confidence and market share, on top of the cost of investigation, remediation, and lost future sales.

Risk that lingers

Because the keys can't be revoked, affected devices stay vulnerable unless their firmware is updated, which isn't always possible.

IN SUMMARY

Keep signing keys in hardware, not on disk

The 2023 MSI theft showed what happens when critical signing keys live outside hardware protection. Firmware signing and Intel Boot Guard keys were stolen and leaked, and because they are fused into devices, the risk can't simply be revoked. CodeSign Secure is built to prevent this: keys are generated and used inside FIPS 140-2 Level 3 HSMs and never exported, signing is automated inside CI/CD and firmware pipelines, access is gated by RBAC, MFA, and quorum approvals, and every signature is logged, timestamped, and compliance-ready, with PQC algorithms for what comes next. Protecting the supply chain starts with keys that can never leave their secure environment.

SEE IT IN ACTION

Keep your signing keys in hardware.

Book a CodeSign Secure demo →