CISO GLOBAL

A **CISO GLOBAL** CASE STUDY

A **CAUTIONARY COLLEGE** Tale

XDR

Attackers love to establish and maintain covert presence in target systems over significant periods of time, extending their opportunity to deeply penetrate the infrastructure, accessing more assets than would otherwise be available to them.

Recently CISO Global was asked by a major university for Incident Response Services following near total loss of their critical infrastructure. College staff and students arrived one morning to find that servers, storage and backups had been deleted, removed or encrypted. Screens across the campus displayed ransomware notes.

Despite having carefully considered its network security and put in place what it believed were the necessary precautions, the university had no way to recover its data or regain access to its systems.

CISO Global was engaged to perform a forensic investigation, ensure no attackers remained in the network, provide remediation, and rebuild systems.

Undercover Attack

The university had no idea adversaries were inside their network, and had been for several months, until they found themselves without access to data and systems. The true extent of the attack only became apparent following CISO Global's investigation.

Making their initial entry via a vulnerability on an unpatched endpoint, the attackers used a widely available utility, Mimikatz, to capture user credentials in real-time. Once an administrator logged in, they had the access they needed.

Over the next three months, they moved freely through the university's systems, performing reconnaissance, setting up repeating scheduled tasks to establish persistence, and executing malicious actions via known good Remote Monitoring and Management (RMM) tools. During this time, they performed gradual data exfiltration. Pilfering the data slowly over time and using known good tools helped keep the attack covert.

AVERAGE COST OF A BREACH

Under 200 days to contain: **$3.61 million**

$4.87 million **Over 200** days to contain:

Source: Cost of a Data Breach, Ponemon, 2021

Detonation

On completing all their planned actions, the attackers detonated their ransomware, leaving the university and its thousands of students locked out of systems for several weeks. The attack resulted in near total infrastructure loss, as well as the exposure of sensitive student data.

It's a sobering story, in part because the attackers used known good tools, thereby completely circumventing the university's antivirus systems. It is, however, a story which could have been significantly shorter and, indeed, near trivial, had the university had the benefit of XDR.

Stopping the Attack

A well configured XDR solution could have stopped the attack, automatically, almost before it began, as soon as Mimikatz was installed.

Even if the attackers had then found an alternative covert way in, XDR's ML-powered behavioral analysis would have identified anomalous behaviors as the attackers used the administrator's credentials to move around the network. It would have alerted SOC analysts who would have stopped the attack immediately.

Similarly, XDR would have spotted the slow data exfiltration to the attackers' online storage as unusual network traffic to a new IP address. It would also have raised alerts on seeing RMM tools installed on endpoints which previously had not hosted them. These are exactly the sorts of behavioral anomalies XDR is built to catch.

By gathering and analyzing information, establishing telemetry across the university's digital estate – endpoints, firewalls, network traffic flows, SaaS and PaaS – XDR would have identified and stopped the attack months before the ransomware was ultimately detonated, saving the university millions of dollars, significant brand damage, extensive data loss and weeks of downtime.

ABOUT CISO GLOBAL

About Us

A leader in cybersecurity and compliance services, CISO Global brings together expert practitioners and thought leaders to provide tailored solutions that drive cyber resilience. The company's top-tier talent spans geographies, specialties, industries, regulatory frameworks, and focus areas and includes auditors, compliance specialists, certified forensics experts, ethical hackers, IEEE®-certified biometric professionals, security engineers, and around-the-clock analysts.

To learn more, visit www.ciso.inc.

AICPA SOC aicpa.org/soc4so SOC for Service Organizations · Service Organizations™

SOC 2® Type II Audited

CISO GLOBAL

480-389-3444 | www.ciso.inc