



razorpoint
SECURITY TECHNOLOGIES

IS IT
SAFE?

RZ.DATAWATCH™

**MULTI-ATTACK DETECTION:
ANTI-PHARMING,
DOMAIN HIJACKING
& MAN-IN-THE-MIDDLE**

WOULD YOU KNOW IF YOU WERE A VICTIM?

www.razorpoint.com/rz.datawatch

Case Study:

On a recent network forensics project, Razorpoint Security was selected to secure a business network that was seized via court order. Razorpoint's role was to provide access to facilitate the legal investigation by attorneys and forensic accountants – the company's senior management had been removed. Razorpoint was able to provide access to all systems, including email. A week

after completing its role, Razorpoint heard the email system had stopped working. Running through a systematic review, Razorpoint ascertained the domain name of the company had been hijacked and email was now being routed to senior management again, outside the company. Razorpoint's expertise was able to assess and document this quickly and move to return the domain name (and all its Internet traffic) to the company's servers.

STEALING YOUR BUSINESS

Imagine Internet traffic sent to and from your servers being relayed through an attacker's server first. All traffic. Email, web pages, file transfers, everything. Would you notice? How? Everything appears to be working normally. Why bother to check? As our case study above illustrates, this attack is real and usually gets discovered after it's too late.

MULTIPLE STEALTHY ATTACKS

The majority of security discussions focus on barriers and keeping attackers "out." But, what if your business could be compromised without anyone ever touching your network?

Pharming, Domain Hijacking and Man-In-The-Middle (MITM) Attacks affect your web site, e-commerce business and email traffic without triggering an intrusion detection system, without ever showing up in a firewall log, and without you knowing.

It is a common misconception that a "hacked site" is one that gets taken down. For cybercriminals, the most lucrative sites are the ones that remain functional and appear to have nothing wrong.

This attack happens to companies both large and small. Conventional security technologies like firewalls, VPNs, SSL encryption, token-based passwords, and intrusion detection/prevention systems are useless in identifying or preventing this type of attack.

RAZORPOINT SECURITY'S RZ.DATAWATCH™

Standard "network monitoring tools" usually observe your network from the inside, and not from the outside the way the world does.

Rz.DataWatch™ analyzes domain names, server information, mail routing data, and 15 other key data points the way the world sees you. Using our methodical data sensors, frequent reviews of your presence online are compared against a locked baseline snapshot of your information. Rz.DataWatch™ routinely monitors your data and identifies malicious activity.

ELIMINATES FALSE POSITIVES

No security tool is beneficial if it just generates more noise. Our data comparison engine is specifically designed to reduce false positives. Razorpoint engineered Rz.DataWatch™ to alert you only when a real issue arises.

EXPIRED DOMAINS

When does your domain name registration expire? Do you know that if you forget to renew your domain name your company can effectively "disappear" from the Internet? Even large companies like Microsoft have fallen victim to expired domain names due to failing to pay the minimal fees to keep a domain alive. Don't worry, Rz.DataWatch™ monitors this for you, too.

REALITIES OF SECURITY

Domain names (the name of your company on the Internet) are registered via companies called registrars. Most registrars provide a web-based interface that allows for changes to contacts, DNS (Domain Name Service) information, and expiration dates. Should an attacker guess or use a variety of other techniques to compromise your password, access to your domain name information becomes vulnerable.

With this type of access, traffic to your domain could be re-routed or stopped completely. Re-routed traffic could be sent through an attacker's servers and then on to yours. This "proxying effect" essentially puts the attacker between you and the rest of the world. They become the "Man In The Middle."

Even SSL-encrypted connections can become useless with this type of attack.

A domain registrar compromise, a server attack, DNS poisoning, or a disgruntled employee are just some of the ways these attacks are achieved.

SECURITY FOR ALL

Rz.DataWatch™ is designed for companies large and small. Rz.DataWatch™ monitors your information with our data sensors reporting any unauthorized changes.

There is no software to install, no web GUI to manage. We do everything. Automatically and unobtrusively.

COMPATIBILITY

Because it is designed to work more effectively than most network monitoring tools, Rz.DataWatch™ is compatible with all servers, operating systems and network appliances.

DOCUMENTATION & CHAIN OF EVIDENCE

Should you need to provide information to law enforcement regarding an attack, Rz.DataWatch™ can be used to document and demonstrate a "chain of evidence" as to how your information existed on the Internet over time.

REGULAR REPORTING

In addition to reporting whenever malicious activity occurs, Rz.DataWatch™ reports monthly with a status of your online information.

DOMAIN NAMES, CONTACTS, EXPIRATION DATES

All of the critical data that keeps your business on the Internet gets reviewed, multiple times, daily. You can think of Rz.DataWatch™ as your business's "online video surveillance system."

FEATURED ON

Our expertise makes Razorpoint Security a prime media source on information security. We have been featured by CNN, CNBC, Forbes, The New York Times Magazine, MSNBC, PC Magazine, Crain's, CBS, Fox5, ABC/CourtTV and many others.



The New York Times Magazine



Forbes



CRAIN'S
NEW YORK BUSINESS



Razorpoint Security Technologies, Inc.