FIELD EFFECT COVALENCE

Key indicators of **security compromise**

On average, it takes six months to detect a data breach and another three to contain it.

Some signs of security compromise are obvious — receiving a threat alert sudden network latency, or finding a ransom note — but there are several subtle clues, too.

By keeping your eyes open for common indicators of compromise (IOCs), you can catch cyber threats early and significantly reduce the damage.

Signs to watch for:

	EMAIL COMPROMISE	MOBILE DEVICE COMPROMISE	HOST OR SERVER COMPROMISE	OTHER
DESCRIPTION	This is a common source of compromise because it is relatively easy for an attacker to execute. All it takes is a convincing phishing email, an email with a malicious script-injected link, or a weak password.	The volume of both personal and professional sensitive information stored on and shared via mobile devices makes them an enticing target. Sources of device breach come in many forms, such as malicious apps and links or even public charging stations.	This is often the main objective of a cyber attack. There are many different types of attacks, with most aiming to get malware onto the host. Generally, the goal is to access and encrypt sensitive data for sale or extortion.	Not every indicator fits into a direct group. There are other signs of compromise.
INDICATORS OF COMPROMISE (IOCS)	• New inbox rules that mark emails as read or move them to a folder, often an RSS folder • Outgoing messages not sent from the legitimate user • Account login or activity from unexpected IP addresses or locations • Corporate messages or accounts listed in online forums • Account login using legacy protocols	• A rapid change in battery drainage • A slow or unresponsive device • Unexpectedly high data usage • New applications not downloaded by the device owner • Unusual or unexpected account activity	• Detection from Windows Defender or another antivirus • Abnormal processes running • Encrypted files and a ransomware note • Event logs indicating uncommon activity • Creation of new admin account • Legitimate admin account locked • Processes communicating to abnormal destinations • Creation of randomized process names and services • Consistently or frequently high CPU usage • Extra binaries or scripts (.dlls, .aspx) in the web server folders	• Network latency • Uncommon traffic patterns (abnormal data volumes or involving foreign destinations) • Client reporting duplicate or suspicious billing • Irregular financial transactions on corporate accounts • Defaced websites

Think you've been compromised? Here's what to do.

After a suspected compromise, you need to act quickly. Every minute a breach goes undetected is another minute the attacker can compromise accounts, infect equipment, and generally cause harm.

Knowing what to do (and what not to do) in the moments after an incident can substantially lower both recovery time and damage. If you think you've been compromised, keep the following in mind.

THINGS YOU SHOULD DO:

- Take a breath and try to remain calm
- Reach out to forensics@fieldeffect.com as soon as possible to begin the response
- Identify the stakeholders who need to be involved
- Consider the chain of custody requirements (ask us if you're not sure!)
- Focus on this order of operations: identify, recover, protect

THINGS YOU SHOULD NOT DO:

- Wait. Even if you're not certain you've been compromised, reach out to us
- Try to cover tracks. This isn't a blame game, and these actions can slow recovery time
- Discuss the incident with someone who is not a direct stakeholder

New and existing clients can connect with us directly to report an incident. No matter the time of day, you can expect a timely response.

Web Form	https://fieldeffect.com/report-an-incident/
Email	forensics@fieldeffect.com
Phone	+1 (800) 299-8986

FIELD EFFECT

We've got your back.
fieldeffect.com

We offer detailed incident response services to identify what happened and how, whether the incident remains ongoing, and a path to recovery. Our comprehensive approach also includes identifying critical vulnerabilities that could present a threat to your organization in the future.

CONTACT US

Email: sales@fieldeffect.com

North America +1 (800) 299-8986

United Kingdom +44 (800) 086-9176

Australia +61 (1800) 43141