How to detect a data breach 1/2

Symptoms of a data breach

- Unusual amount of requests within a time frame.
- Large amount of failed logins from a single user.
- Large amount of failed logins for multiple users from same IP address - although this can be really tricky because of NAT implementations.
- Someone logging in during strange hours or at strange locations. Pay attention to admin accounts. Of course, sometimes locations and times vary because of business trips and time zone changes, or due to working overtime, which may cause false positives.
- Strange input patterns and suddenly, a lot of input validation failures.
- Sudden peaks of network activity.
- Traffic to/from unusual ports. What's unusual, depends of course on the set of services you provide. Skype, and various instant messaging software can cause a lot of false positives.
- Traffic to blacklisted or known malware domains and URLs.
- Strange TLS certificates used in TLS connections.
- Changes in DNS records.
- Sudden peaks in CPU or memory consumption.
- Lost connection to monitored hosts.

How to detect a data breach 2/2

Symptoms of a data breach

- New files appearing to your file system in certain directories. If the server's purpose is to be a file server or multi-user web server, this causes a lot of false positives.

- New files with .js, php, or .html extensions appearing which use base64_decode, eval, preg_replace, substr, gzinflate, or similar functions often used by exploit kit type of malware. Grepping for these regularly is a good idea.

- High entropy in .js, php, or .html files often implies obfuscated code or base64 encoded data blobs. Minified JavaScript files often cause false positives.

- Weird or non-existing User Agents and other headers. This is a very likely source of false positives, so creating alerts based on this is not a good idea. However, this can be sometimes used as a last of line of checks.

If you suspect a data breach:

1. Do not panic.

Start keeping record of your actions. This ensures that in later stage you can differentiate your actions from the perpetrator's actions.

2. Do not shut down potentially compromised computers

Do not shut down potentially compromised computers and try to avoid using them if possible. Do not run antivirus checks or similar.

3. If necessary (cryptomalware, active data leakage or similar cases), disconnect potentially compromised computers from the network, or isolate them from rest of the environment using firewall.

Before disconnecting systems from network make sure what effects there might be. Damages from uncontrolled shutdown might be more severe than damages from the original compromise.

4. Collect all background information about the incident and potentially compromised computers.

- What happened, where and when?
- What is the role of the computers?
- Who owns the computers and can make decision regarding them (i.e. shut down a service)

5. Contact your organization's information security team or call Nixu directly +358 40 821 6432.

If you are Nixu CSIRT customer, please use your organization's dedicated number.

nixu cybersecurity.