

# Scenario



**A supplier of your HRM software was targeted and a backdoored version was distributed. You may already upgraded. Indicators of compromise were published.**

# Scenario



Your national CERT has published some indicators of compromise for your country and specifically for your industrial sector. Report back if you found hits.

# Scenario



Different employee accounts were abused for further attacks against your customers. During initial analysis, you found that all of them visited a typo domain of your corporate portal.

# Scenario



An employee's workstation was infected with a banking Trojan which not only changed network settings but also installed email monitoring software. It is related to a recent malvertising campaign.

# Scenario



You are notified that one of your ticketing systems is compromised and malware was placed on that server. It connects to other systems reachable from the ticketing server.

# Scenario



**Spear phishing attack against an employee and employee reports login in into a similar looking company portal.**

# Scenario



**Spear phishing attack against an employee using a malicious document which after it was opened executed code on the computer.**

# Scenario



Employee downloads a malware through a fake software package which connects back to command and control servers using DNS.



# Scenario



Vulnerability was exploited on one of your servers and an attacker had access to the database with customer data. A increased bandwidth was registered on the network device.

# Scenario



A database with customer data was exposed to the Internet through a misconfigured firewall and someone on Twitter is leaking data from that database.

# Scenario



A public git repository leaked internal credentials and it's unclear whether the credentials were already abused.

# Scenario



**Servers from your main online  
service were targeted by a DDoS  
and are unavailable.**

# Scenario



Malicious code was distributed to your endpoints during the routine update of a signed application.

# Scenario



A domain admin has run a malicious attachment after loudly proclaiming how dumb their users are for doing the same.

# Scenario



Security company has released an APT group PDF at BH USA. The list of IOCs includes a host in your ASN.

# Scenario



**Every night new corporate accounts  
are abused for sending spam.**



# Scenario



Email infrastructure got  
compromised. Attackers have full  
access to your mailboxes.

# Scenario



**Attackers got domain admin in your environment. What should you scary more? Backdoor accounts or the sudden activation of disk encryption software?**

# Scenario



**An adversary has access to your  
Jenkins server.**

# Scenario



An adversary has access to your vulnerable Jenkins server. Jenkins jobs with credentials are visible to everyone.

# Scenario



**Someone is impersonating you to  
customer support.**

# Scenario



Your DNS was modified to respond  
with an attacker's DKIM key.

# Scenario



Due to a botched CI/CD script,  
complete source code exposure on  
production.

# Scenario



A bug in your webapp has allowed every record to be accessed via URL enumeration and IDOR.



# Scenario



**Your subscription database is  
hacked. Thousands of new accounts  
are added and hard to distinguish  
from old.**

# Scenario



New paste on a public paste site was found with password hashes and emails from your customer DB from 3 years ago. More recent hashes are missing.

# Scenario



Your reception software has leaked  
all of your visitor logs. They are  
available via torrent.

# Scenario



A script has been logging exported variables containing full user registration objects. This logging method is full of plaintext passwords.

# Scenario



Joker - be evil and invent a new nightmare and worst case scenario. What scenario will get your team struggling? (If you want to get crazy then contribute your scary scenario for the sake of humanity.)

# Scenario



Joker - be evil and invent a new nightmare and worst case scenario. What scenario will get your team struggling? (If you want to get crazy then contribute your scary scenario for the sake of humanity.)

# Scenario



Joker - be evil and invent a new nightmare and worst case scenario. What scenario will get your team struggling? (If you want to get crazy then contribute your scary scenario for the sake of humanity.)

# Scenario



A developer has just typo'd an upstream package installation to their laptop. There was a malicious package waiting for that typo and post-installation code is exfiltrating data.



# Scenario



An engineer has typo'd a package they are adding to a product repository. It is malicious. The CI/CD and prod environment variables are exfiltrated to a C&C

# Scenario



A malicious browser extension was installed on different corporate computers. It injects keyloggers into websites.

# Scenario



Your build imports from an employee's personal NPM package. They quit, and vandalize the package, causing a public incident.

# Scenario



An adversary takes control of your MDM service account. Your MDM support team cannot be reached for account recovery.

# Scenario



Your DNS was modified to respond  
with an attacker's DKIM key.  
Spearphishes will be signed by your  
domain in 30 minutes.

# Scenario



The certificates involved with your primary code signing process have been compromised and used to sign malicious apps.

# Scenario



An employee has left a firewall rule wide open after several hours of troubleshooting a network issue.

# Scenario



An employee has left a firewall rule wide open after a faulty change request was implemented. Bruteforcing attempts were registered on previously protected servers.



# Scenario



You allow customers to upload sensitive information to your platform to share them with others. However, the data was left unprotected and anyone could access and download the content.

# Scenario



**You were informed that one of your website directories used to share files with external parties were accessible and writable by any anonymous user. Suspicious files were found.**