

**<Company Name>**

**Cyber Security Team Blue Team XX**

Blue Team XX

*<Company Name> Cyber Security Team*

*<Company Location>*

<Recipient Name>

NECCDC

<Recipient Location>

**March X, 2023**

Dear <Recipient>,

Below, you will see our report regarding a recent **incident** that had occurred.

Thank you,

Blue Team XX

General Information

| **Team Number:** |
| --- |
| **Time of Incident (Include time zone):** |
| **Status:**   * Site Under Attack * Incident Investigation In Progress * Incident Closed |
| **Department Affected:** <e.g File Management> |
| **Type of Incident:**   * Malicious code: virus, Trojan horse, worm * Probes / scans (non-malicious data gathering - recurring, massive, unusual) * Attack (successful/unsuccessful intrusions including scanning with attack packets) * Denial-of-service event * High embarrassment factor * Deemed significant by site |
| **Severity:**   * Minimal * Moderate * Severe * Catastrophic |
| **Executive Summary:** |

Business and Infrastructure Impact

| **Services affected:** <website server, API functions, email server> |
| --- |
| **Was any sensitive information leaked?**   * Yes * No |
| **If yes, specify what *type* of data was leaked:** |
| **Has any data been changed?**   * Yes * No |
| **If yes, specify what *type* of data was changed:** |
| **Damage done:**   * Numbers of systems affected: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * Nature of loss, if any: \_<environmental, human>\_\_\_\_\_\_\_\_ * System downtime: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Additional Contacts:**   * Law Enforcement: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * Other : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Internal services affected**: <VPN server, Employee database> |
| **Recoverability:** |
| **Cost of incident:**   * Unknown * None * <$10K * $10K-50K * >$50K |

Technical Details

| **Time First Identified:** |
| --- |
| **Time Last Identified:** |
| **Apparent Source:**   * <If DoS or DDoS and which IP(s) it came from> * <Specify if the attack was domestic, foreign, or insider if scan or DoS> * <If malicious software, specify which piece of software. Downloaded from online? Attach link> |
| **Primary system or network involved:**   * IP addresses (full) or subnet addresses (CIDR): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * Hostname: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * OS version(s): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * NOS version(s): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Root Cause of Incident:** |
| **Other affected systems or networks (IPs and OSs):** |
| **What under the system or network was affected (user, file, etc):** |
| **Attack Vector:** (<https://attack.mitre.org/>) / IOCs |
| **How was the attack carried out specifically?**  <Based on the root cause, how did this happen?>  <If data exfiltration, and you know where, say here> |
| **Level of access gained?** (Root / administrator, other user, domain controller admin) |
| **How was the attack detected?** |
| **Remediation steps taken:** |
| **Corresponding logs:** |
| **Other supporting artifacts:** |
| **Lessons Learned / Opportunity for Improvement:** |