

**<Company Name>**

**Cyber Security Team Blue Team XX**

Blue Team XX

*<Company Name> Cyber Security Team*

*<Company Location>*

<Recipient Name>

NECCDC

<Recipient Location>

**August X, 2024**

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 Discovery (Include time zone):** |
| **Severity:**   * Minimal * Moderate * Severe   Catastrophic |
| **Status:**   * Site Under Attack * Incident Investigation In Progress * Incident Closed |
| **Service Affected:** <e.g File Management>  **Primary system or network involved:**   * IP addresses (full) or subnet addresses (CIDR): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * Hostname: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * OS version(s): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * NOS version(s): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Was any sensitive information leaked?**   * Yes * No |
| **Executive Summary:**  **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  **Has any data been changed?**  **If yes, specify what *type* of data was leaked:**  Yes  No    **Recoverability:** |

Technical Details

|  |
| --- |
| **Root Source/Root Cause:**   * <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> |
| **Attack Vector:** (<https://attack.mitre.org/>) / IOCs |
| **Level of access gained?** (Root / administrator, other user, domain controller admin) |
| **What actions did they attackers take?**  <Based on the root cause, how did this happen?>  <If data exfiltration, and you know where, say here> |
| **How was the attack detected?** |
| **Corresponding logs:** |
| **Remediation steps taken:**  **Lessons Learned / Opportunity for Improvement:** |
| **Other supporting artifacts:** |