

**<Company Name>**

**Cyber Security Team Blue Team XX**

Blue Team XX

*Placebo Pharma Cyber Security Team*

*Bristol, Rhode Island*

<Recipient Name>

NECCDC

<Recipient Location>

**March X, 2025**

Dear <Recipient>,

Submit IR reports when incidents occur in order to potentially reduce future Red Team impacts

Must contain a description of what occurred (including source and destination IP addresses, timelines of activity, passwords cracked, access obtained, damage done, etc), a discussion of what was affected, and a remediation plan.

This report details red team activity on our < Linux / Windows / Kubernetes > systems first identified at <Date / Time / Time Zone>. We are still < under attack / investigating / resolved > as of <time last seen>.

This was a < Minimal / Moderate / Severe / Catastrophic > incident, and attackers had < remote access / root access / data access > to our systems. We were able to < fully / partially / not > recover control of the affected systems.

< Identify impacts on business >

<Summarize incidents X, Y, Z>

< Summary doesn’t include ‘Figures’ or a huge amount of technical detail >

Section X: Reverse Shells

Affected systems: < X1 IP, Graylog Master: 192.168.0.1, X3 IP>

Severity: < Minimal / Moderate / Severe / Catastrophic >

Indicators of Compromise:

<There were 8 reverse shells identified on the system, as seen in Figure 1. The shells gave attackers remote access to our systems, and resulted in a total compromise of the affected systems.>



Figure 1: This cat is pretty cool. We found it through a ps aux listing

< These shells were started by .bashrc, which means they ran on every login for user100. We found it in every user’s .bashrc file. >



Figure 2: Bashrc output, showing command used

Remediation:

< We removed this access by deleting the relevant .bashrc lines (Figure 3), killing all reverse shells (Figure 4), and confirming no reverse shells were made on subsequent logins (Figure 5).

This has been fully remediated. >

Business Impact:

< attacker access to the system puts all client data at risk>

Lessons Learned:

< I learned nothing. >

Section Y: TacticalRMM

Affected systems: < X1 IP, Graylog Master: 192.168.0.1, X3 IP>

Severity: < Minimal / Moderate / Severe / Catastrophic >

Indicators of Compromise:

Remediation:

Business Impact:

Lessons Learned: