Purpose

This sample report outlines key sections of deliverables associated with technical documentation and tracking of an incident during all phases of incident response, including detection, containment, eradication, recovery and lessons learned.

Proprietary and confidential

<Name, Role>
<Date of the report>

Contents

Incident Summary

- How the incident was detected, including timeline.
- What is the source of the attack, critical attack path and potential motivation?

- What is the method/tactic of the attack (malware, malicious document, and other adversary tactics or agents)?

Information exposure

- What information was breached/accessed/stolen and impact with respect to operations, teaching or research?

Investigative findings

Incident Timeline

Sequence of the events leading to the detection of the compromise

Key events in timeline

Time (EDT)	Description

Incident Analysis

Malware and miscellaneous files connected to the compromise

Name	Location/File Path (include MD5 hash, owner, and size)	Purpose

Extent of the compromise

List of assets (compromised, suspected to be compromised, clean). This includes devices such as servers, workstations and laptops, user accounts, services, applications, etc. …

Infected servers, workstations, user accounts, services, etc. …

Server	IP address	Purpose	Remediation Date	Status
Server 1		Mail server	June 2, 2018	Turned off
Server 2		File server	June 5, 2018	Forensic analysis
Server 3		Virtualization server	June 2, 2018	Isolated
Workstation 1		RDP client's station	June 2, 2018	Turned off

Workstation 2		Batch job workstation	June 2, 2018	Retired

Containment

- Content to be added here.

Preservation of evidence

- Engagement of the forensic company
- Forensic image of disk
- Collection of logs
- Documentation of the environment (network topology, system architecture, etc. …)

Remediation

- Content to be added here.

Further work

- Content to be added here.

Lessons learned

- Content to be added here.

Appendix

Supporting Files (to be uploaded)

File name	Description