Text, logo

Description automatically generated with medium confidence

­­

Incident Response Report

<Client Full>

CONFIDENTIAL/PRIVILEGED



<IR2Y-XXXX>

<DD Month YYYY>

Legal Acknowledgements

## **Copyright**

©Copyright 2021 IBM Corporation. All Rights Reserved. This is unpublished material and contains confidential information and is subject to a confidentiality agreement. The unauthorized possession, use, reproduction, distribution, display, or disclosure of this material or the information contained herein is prohibited.

The methodologies and processes used in the conduct of this engagement are considered proprietary intellectual property of IBM and may not be disclosed without written permission from IBM. IBM authorizes you to copy this report for the purposes of disseminating information within your organization or any regulatory agency.

## **Confidentiality**

This document contains confidential information of a proprietary and sensitive nature. As such this document should be afforded the security and handling precautions that a confidential document warrants. This document should have a controlled distribution to relevant parties only and should not be copied without written permission.

IBM treats the contents of any Emergency Response Services (IBM) engagement as confidential material and will not disclose the contents of this document to anyone without written permission.

## **Disclaimer**

New technology, configuration changes, software upgrades and routine maintenance, among other items, can create new and unknown security exposures. Moreover, computer “hackers” and other third parties continue to employ increasingly sophisticated techniques and tools, resulting in ever-growing challenges to network and computer system security. The Report and the recommendations contained herein do not constitute any representation or warranty by IBM about the security of a company’s network and/or computer systems including, but not limited to, any representation that a company’s computer systems are safe from intrusions, viruses, or any other security exposures.

# Document Control

**Reviewers**

|  |  |  |
| --- | --- | --- |
| Date | Current Version | Name |
| 06 August 2021 | Prepared by | S Kodź |
| 06 August 2021 | Reviewed by | B Sen |
| DD Month YYYY | Approved by | <manager approval> |

**Change Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Status-Description | Author |
| 06 August 2021 | 0.1 | Initial Draft | S Kodź |
| DD Month YYYY | 0.2 | Initial Draft | <author> |
| DD Month YYYY | 1.0 | Final Draft | <author> |

Table of Contents

[**Copyright** 2](#_Toc79157245)

[**Confidentiality** 2](#_Toc79157246)

[**Disclaimer** 2](#_Toc79157247)

[Document Control 3](#_Toc79157248)

[Executive Summary 6](#_Toc79157249)

[Background 6](#_Toc79157250)

[Summary of XFIR Response and Analysis Conducted 7](#_Toc79157251)

[Summary of Findings 7](#_Toc79157252)

[Incident Timeline Summary 7](#_Toc79157253)

[Background 8](#_Toc79157254)

[Incident Declaration 8](#_Toc79157255)

[Incident Details 8](#_Toc79157256)

[Engagement 8](#_Toc79157257)

[Data Collection and Preservation 9](#_Toc79157258)

[Evidence Sources 9](#_Toc79157259)

[Data Acquisition 9](#_Toc79157260)

[Property Disposition 10](#_Toc79157261)

[Forensic Analysis and Findings 11](#_Toc79157262)

[SystemOne 11](#_Toc79157263)

[System Information 11](#_Toc79157264)

[Event Logs 11](#_Toc79157265)

[Windows Registry 11](#_Toc79157266)

[Keyword Search 11](#_Toc79157267)

[File System 12](#_Toc79157268)

[System Two 12](#_Toc79157269)

[System Three 12](#_Toc79157270)

[Data Log Source(s) 12](#_Toc79157271)

[Findings 13](#_Toc79157272)

[Recommendations 14](#_Toc79157273)

[<Recommendation 1> 14](#_Toc79157274)

[<Recommendation 2> 14](#_Toc79157275)

[<Recommendation 3> 14](#_Toc79157276)

[<Recommendation 4> 14](#_Toc79157277)

[Appendix A. Incident Timeline 15](#_Toc79157278)

[Appendix B. Indicators of Compromise 16](#_Toc79157279)

[File Based Indicators of Compromise 16](#_Toc79157280)

[Network Based Indicators of Compromise 16](#_Toc79157281)

[Appendix C. Compromised Accounts 17](#_Toc79157282)

[Appendix D. Malware Analysis 18](#_Toc79157283)

[Appendix E. List of Keywords Searched 19](#_Toc79157284)

[Appendix F. Additional Documents 20](#_Toc79157285)

# Executive Summary

This report presents findings and recommendations resulting from investigative activities performed by IBM Security X-Force Incident Response (‘XFIR’) on behalf of (‘’).

All dates and times listed in this report are in UTC time zone and time format is based on 24-hour system, e.g. 23:54. Short format dates are in the format YYYY-MM-DD.

## Background

On DD Month YYYY at hh:mm, of contacted XFIR to report a suspected incident concerning the environment.

Following a triage call, that XFIR hosted on DD Month YYYY at hh:mm:ss, XFIR’s understanding of the incident is <high level synopsis of circumstances>

e.g. <client> personnel identified Symantec Endpoint Protection alerts related to credential harvesting utilities originating from three <client> servers between 15 August and 29 August 2018. <client> personnel performed an initial investigation into the activity but were unable to identify the root cause for the Symantec Endpoint Protection alerts nor were they able to determine the accounts responsible for the alerts.

<person> stated <client> information security personnel did not identify any additional suspicious activity within the <client> environment.

On , engaged XFIR perform a forensic investigation, the objectives of which were to:

1. Determine the root cause of the Symantec Endpoint Protection alerts for the credential harvesting utilities and the user accounts associated with the activity;
2. Determine if there is evidence of a network intrusion into the environment and if so, the extent of the compromise;
3. Provide necessary containment and remediation recommendations to assist with resolving the potential incident; and
4. Provide recommendations on detecting future incidents and mitigating their impact to business operations.

The in-scope timeframe for this investigation, as agreed with is DD Month YYYY to DD Month YYYY.

< IF REQUIRED >

During the course of the investigation it was identified that <circumstances>, based upon this additional information the scope of XFIR tasking was increased to include:

1. Determine the root cause of the Symantec Endpoint Protection alerts for the credential harvesting utilities and the user accounts associated with the activity;
2. Determine if there is evidence of a network intrusion into the <client> environment and if so, the extent; and
3. Save the day.

## Summary of XFIR Response and Analysis Conducted

XFIR established a cloud-based <EDR product> instance and deployed agents to <total> systems in the <Client> environment.

On <DD Month YYYY>, XFIR personnel attended site at <Client> <offices/headquarters/location> in <location> and performed onsite incident response and investigative activities.

XFIR performed forensic analysis of <total> forensic images and <total> memory images from compromised systems or systems of interest.

## Summary of Findings

During the course of the investigation, XFIR performed forensic analysis on historical log data and images of systems provided for analysis. XFIR leveraged X-Force and 3rd party threat intelligence while incorporating analysis from various points of data and determined the following high-level points of significant malicious or suspicious activity.

## Incident Timeline Summary

The timeline below provides a high-level overview of XFIR and malicious actor(s) activities as set out in the previous section, *Summary of Findings*.

|  |  |  |
| --- | --- | --- |
| Date/Time | Event | Description |
| YYYY-MM-DD hh:mm:ss | Vulnerability Announced | Security researcher release a blog stating that a hard-coded password was identified within the application AV Manager for Windows. The blog location is https://www.hacking-by-numbers.com/AV-Manager.html |
| YYYY-MM-DD hh:mm:ss | Malicious Login Identified | Windows Event Logs recorded a login to the ‘manager’ account from public IP address ‘123.45.67[.]89’. |
| YYYY-MM-DD hh:mm:ss |  |  |
| YYYY-MM-DD hh:mm:ss |  |  |

Table 1 - High Level Summary of Important Events

A complete timeline of all events identified for this incident are listed in *Appendix A Incident Timeline*.

# Background

Background information concerning this investigation is as follows:

## Incident Declaration

On <DD Month YYYY at hh:mm>, of contacted XFIR to report a suspected incident concerning the environment.

## Incident Details

XFIR understands <high level synopsis of circumstances>

## Engagement

On , engaged XFIR to perform a forensic investigation, the objectives of which were to:

1. Determine the root cause of the Symantec Endpoint Detection alerts for the credential harvesting utilities and the user accounts associated with the activity;
2. Determine if there is evidence of a network intrusion into the environment and if so, the extent of the compromise;
3. Provide necessary containment and remediation recommendations to assist with resolving the potential incident; and
4. Provide recommendations on detecting future incidents and mitigating their impact to business operations.

# Data Collection and Preservation

In the course of this investigation XFIR captured and took receipt of various evidence sources. Examination of this evidence was the foundation of the investigation in addition to various stakeholder interviews. During the course of the engagement, XFIR performed forensic analysis on three (3) forensic images acquired from systems related to the incident. XFIR and <Client> personnel worked together to establish access and procedures for secure acquisition and transfer of the required data. Details of the evidence captured and/ or analysed is detailed in the sections which follow.

## Evidence Sources

System images captured and/or analysed during the course of this investigation were as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Hostname | Type | Media ID | Image Name | MD5 Hash |
| JIMMY-WIN7 | Disk Image | IR21-XXXX\_hostname | JIMMYC-WIN7.E01 | 756E088BD13AFAFB0106BA97CCC56545 |
| BOB-WIN10 | Disk Image | IR21-XXXX\_hostname | svaddc03\_apr5\_1-flat.vmdk | AFAE36608D2F76CAACC2D672F8D4DE43 |
| SVADDC03 | Memory Image | IR21-XXXX\_hostname\_01 | SVADDC03-Snapshot55.vmem | D37CDC9F5CCD28F0B93EE37F88211F9B |

Table 2 - Evidence Collected and Analysed

Log data captured and/or analysed during the course of this investigation was as follows:

|  |  |  |
| --- | --- | --- |
| File Name | Description | MD5 Hash |
| somefilename.tar.gz | <type> logs from <device> for period YYYY-MM-DD to YYYY-MM-DD captured by XFIR. | 756E088BD13AFAFB0106BA97CCC56545 |
| data.7z | <type> logs from <device> for period YYYY-MM-DD to YYYY-MM-DD provided by <customer>. | AFAE36608D2F76CAACC2D672F8D4DE43 |

Table 3 - Logs Collected and Analysed

Other evidence sources captured and/or analysed during the course of this investigation were as follows:

|  |  |  |
| --- | --- | --- |
| File Name | Description | MD5 Hash |
| Golden Image | Golden Workstation Image | 756E088BD13AFAFB0106BA97CCC56545 |
| Backup File | Backup of Domain Controller | AFAE36608D2F76CAACC2D672F8D4DE43 |

Table 4 - Other Evidence Sources Collected and Analysed

## Data Acquisition

<detailed data acquisition information>

<describe the background to the data collected, its methods, and who performed what>

e.g. All the disk images listed in *Table 2* above were collected by personnel, following instructions supplied by XFIR. Data was captured using FTK Imager version 4.2.1.4 as a live capture to USB media attached to the device.

The memory image was captured by personnel, following instructions supplied by XFIR, using FTK Imager version 4.2.1.4. The memory capture was saved directly to USB media attached to the device.

Log files for the in-scope timeframe were exported by personnel using the built-in functionality withing in the firewall management graphical user interface. Once exported, the MD5 hash was calculated using the PowerShell command ‘Get-Filehash’ and recorded in a text file, that was supplied to XFIR with the exported log data.

## Property Disposition

The aforementioned evidence sources were collected and secured by XFIR <or> The aforementioned evidence sources were collected by and secured by XFIR. Final disposition of all materials via IBM Property Control Document will be coordinated with upon completion and acceptance of this written report.

# Forensic Analysis and Findings

This section describes in detail the findings from each investigated system. It contains results from full disk image analysis of systems listed in *Evidence Sources* as well as data extracted directly by XFIR from CBR, deployed for this investigation.

XFIR identified several malware samples and non-malicious tools used by attacker. Since these were repeatedly used across multiple systems, XFIR analysis related to identified malware has been document in *Appendix D Malware Analysis*.

## SystemOne

Provide a brief explanation as to why this system has been included within the scope of work. For example: This domain controller has been included within the investigation as Client (short) identified the domain administrator account had logged onto the server.

### System Information

|  |  |
| --- | --- |
| System Information |  |
| Version | Windows Server 2012 R2 Standard |
| Installed Date | 2020-04-17 |
| Computer Name | XXXXXX |
| Last Shutdown | 2020-07-14 |
| IP Address | 10.0.0[.]0 |

Table 5 - SystemOne – System Information

### Event Logs

Windows Event Logs from the system were analysed to identify any suspicious activities related to logons, services, program executions and system operations around the in-scope period.

The available entries in the Windows Event Logs partially covered the in-scope timeframe. The date ranges for the analysed logs are listed below:

|  |  |  |
| --- | --- | --- |
| Windows Log | Start Date | End Date |
| Security | 2020-07-13 | 2020-07-14 |
| System | 2020-04-27 | 2020-07-14 |
| Microsoft-Windows-PowerShell Operational | 2020-04-17 | 2020-07-14 |

Table 6 - SystemOne – Log Information

### Windows Registry

Windows Registry files from the system were analysed to identify any suspicious executions, installed programs or programs set to run automatically, which may have been created or modified around the in-scope timeframe.

There were no further relevant findings within the available evidence.

### Keyword Search

XFIR performed keyword searches for several keywords to discover general command execution. A full list of keywords used for searching is available in *Appendix E List of Keywords Searched*.

There were no further relevant findings within the available evidence.

### File System

A review of files created or modified on or around the in-scope timeframe was undertaken.

|  |  |  |  |
| --- | --- | --- | --- |
| File Name | Full Path | Created | MD5 Hash |
| host.dll | C:\Users\Public\Music\host.dll | 2021-05-10 04:59:48 | A3560DA879904D44BDD76987C1E504F8 |
| 1486r.exe | C:\Users\Public\1486r.exe | 2021-05-11 03:46:27 | C7F866C3476C0B047D4C583151A47CD4 |
| 1063r.exe | C:\Users\Public\1063r.exe | 2021-05-11 03:48:50 | C7F866C3476C0B047D4C583151A47CD4 |

Table 7 - SystemOne – Files of Interest

There were no further relevant findings within the available evidence.

## System Two

OK

Graphical user interface, application

Description automatically generated

Figure 1 - Example of a Figure

## System Three

OK

## Data Log Source(s)

Placeholder for SIEM, Network logs etc.

# Findings

Based on the analysed evidence, XFIR found <main findings e.g. no evidence of malware or malicious activity on the in-scope systems/ evidence of an active compromise of the in-scope systems>

The following was identified as it concerns this incident:

* <Finding 1>
* <Finding 2>

# Recommendations

Based on observations during onsite and remote analysis, XFIR provides the below recommendations.

Many of these recommendations were implemented during the remediation effort of the investigation. As with any changes, these recommendations should be evaluated for applicability and overall effect to the operating environment.

## <Recommendation 1>

<Recommendation>

## <Recommendation 2>

<Recommendation>

## <Recommendation 3>

<Recommendation>

## <Recommendation 4>

<Recommendation>

1. Incident Timeline

The table below provides a complete timeline of notable events showing XFIR and malicious actor(s) activities. This timeline pulls together the findings from all the evidence that has been analysed for this incident.

|  |  |  |
| --- | --- | --- |
| Date/Time | Event | Description |
| YYYY-MM-DD hh:mm:ss |  |  |
| YYYY-MM-DD hh:mm:ss |  |  |
| YYYY-MM-DD hh:mm:ss |  |  |
| YYYY-MM-DD hh:mm:ss |  |  |

Table 8 – Timeline of Notable Events

1. Indicators of Compromise

File Based Indicators of Compromise

The table below contain all the file based indicators of compromise identified during this investigation.

|  |  |
| --- | --- |
| File Name | MD5 Hash |
| host.dll | A3560DA879904D44BDD76987C1E504F8 |
| 1486r.exe | C7F866C3476C0B047D4C583151A47CD4 |
| 1063r.exe | C7F866C3476C0B047D4C583151A47CD4 |

Table 9 - File Based Indicators of Compromise

Network Based Indicators of Compromise

The table below contain all the network based indicators of compromise identified during this investigation.

|  |  |
| --- | --- |
| Domain/URL/IP Address | Details |
| 104.21.29[.]42  172.67.148[.]93 | Command-and-control (C2) domain and resolved IP addresses. |
| 207.102.109[.]106 | Source IP address connected to Citrix NetScaler. |

Table 10 – Network Based Indicators of Compromise

1. Compromised Accounts

The list below contains all the account identified to have been compromised. XFIR generated this list during the incident investigation.

* Account1
* Account2
* Account3
* Account4

1. Malware Analysis

As provided by XFTI – make sure this uses the same template/formatting. ***Failure to submit the report with correct formatting will see it being returned for correction***.

1. List of Keywords Searched

The list below contains the keywords that have been used for searches throughout this investigation. Not all keywords will have been applied for each search.

* Keyword1
* Keyword2
* Keyword3
* Keyword4

1. Additional Documents

The following documents will be included with this report and as such should be considered an important part of the report. The have been included separately for readability, size or otherwise being unsuitable to be included inline within this report.

|  |  |  |
| --- | --- | --- |
| File Name | Description | MD5 Hash |
| image1.png | Screenshot of malicious actor(s) opening files during a recorded remote support session. | A3560DA879904D44BDD76987C1E504F8 |
| video1.mp4 | Complete recorded remote support session. | C7F866C3476C0B047D4C583151A47CD4 |

Table 11 – Files Supplied with the Report

© Copyright IBM Corporation 2021

IBM Security  
Route 100  
Somers, NY 10589  
U.S.A.

Produced in the United States of America  
February 2021  
All Rights Reserved

IBM, the IBM logo, ibm.com, and IBM X-Force are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at: ibm.com/legal/copytrade.shtml

Other product, company or service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not  
imply that IBM intends to make them available in all countries in which IBM operates.