Incident Response Preliminary/Final Report

Lee Sult

404.913.5101

Lee.Sult@nuix.com

CLIENT CONFIDENTIAL

This document is intended for the internal use of recipients only and may not be distributed externally or reproduced for external distribution in any form without express written permission of Nuix and

# Document Control and Distribution

|  |  |  |
| --- | --- | --- |
| Version | Author | Date of Revision |
| 1 |  | 8/10/2015 |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| Project Contact | Contact Name | Contact EMAIL |
|  |  |  |
|  |  |  |
|  |  |  |

Contents

[Document Control and Distribution 2](#_Toc402850928)

[Executive Summary 4](#_Toc402850929)

[Scope 6](#_Toc402850930)

[Incident Background 7](#_Toc402850931)

[Network Topology 7](#_Toc402850932)

[Data Flow 8](#_Toc402850933)

[Analysis 9](#_Toc402850934)

[Data Collection 9](#_Toc402850935)

[Findings 10](#_Toc402850936)

[Initial Findings 10](#_Toc402850937)

[Memory Analysis 10](#_Toc402850938)

[Registry Analysis - Table 1 10](#_Toc402850939)

[Registry Analysis - Table 2 11](#_Toc402850940)

[Log Analysis 11](#_Toc402850941)

[Timeline Analysis 14](#_Toc402850942)

[Database Analysis 14](#_Toc402850943)

[Malware Analysis 15](#_Toc402850944)

[Attack Origination 15](#_Toc402850945)

[Recommendations 16](#_Toc402850946)

[Customer Actions 16](#_Toc402850947)

[Appendix 18](#_Toc402850948)

[Report Contacts 18](#_Toc402850949)

# Executive Summary

The following report is based on the results of an Incident Response Investigation performed by Nuix on dd mmm yyyy

Nuix was engaged on dd mmm yyyy by when \*how and when client discovered suspected breach\*

Prior to engaging Nuix, performed the following actions to investigate and/or remediate the suspected breach:

Action 1

Action 2

Action 3

The initial scope of the investigation was defined as follows:

One (1) Web Server

One (1) Domain Controller

Three (3) Network devices

The initial scope was determined through interviews with key personnel, the completion of an Incident Response Triage Worksheet and a review of the Network Topology.

The goal of the Incident Response Investigation was to determine:

* The means by which the intruder gained access to the <CLIENT> environment
* What data was/was likely targeted by the intruder
* How the intruder moved from the point of entry, to the location of the target data
* The mechanism by which the intruder harvested the targeted data
* How the targeted data was moved from a system controlled by <CLIENT>, to a system controlled by the intruder

Based on these goals, Nuix identified conclusive evidence of a data breach/ No evidence of a data breach.

Report any limitations to the investigation such as missing logs, lack of access, weak retention, etc…

<Report Narrative> Report your facts and be sure that everything you report as fact is backed up by evidence shown in the rest of the report below.

\*SAMPLE\*

On November 8, 2014, an attacker accessed the Client Web Server "Client CF-1" via an attack against the Adobe ColdFusion 9.1 administrative interface. Once the attacker gained access, malware (an administrative webshell) was uploaded to grant the attacker further control of the server. The malware was then used to obtain SSL certificates, cached credentials and a full copy of the stored databases.

The attacker then used the Web Server as a pivot point and attacked the Domain Controller "Client-DC1" via the SMB protocol and the PSExec utility. The attacker was able to add a new account in the "Domain Administrators" group and subsequently infect….

The compromise was contained on 11 Dec 2014 when "Cllient-CF-1" was taken offline and replaced with "CLIENT-CF-2" and a known good backup of the web site. Prior to re-deployment, Adobe ColdFusion was updated to the latest version and all patches were installed.

Although the compromise has been contained, Nuix found other network and system security deficiencies that should be remediated to further secure the network within

# Scope

The investigation scope was determined through interviews with key personnel, the completion of a triage worksheet and a review of the network topology.

Initial Investigation scope was defined as follows:

* One (1) Web Server
* One (1) Domain Controller
* Three (3) Network devices

During the investigation, evidence located on "Device Name" led to an expansion of scope.

\*EXPLANATION\*

List of items added to scope

* Device
* Device
* Device

# Incident Background

This section of the report contains information pertaining to why Nuix was engaged to perform an investigation, basic data about CLIENT network topology and data flows.

CLIENT is a XXXX business and maintains a Corporate/Small Business/Ecomm/POS environment for the purpose of X. On DDMMMYYYY, CLIENT noticed X, X and X which led to the launch of an investigation.

OR

On DDMMMYYYY, CLIENT was notified by X that data belonging to CLIENT was discovered at LOCATION X. Confirmation of this data leak led to the launch of an investigation.

## Network Topology

The following diagrams represent a high-level overview of the network operating environment at CLIENT LOCATION.





## Data Flow

The following diagrams represent a high level overview of the data flow inside of the CLIENT NETWORK LOCATION.

<INSERT DIAGRAM>

DATA SUSPECTED OF BEING BREACHED is entered (1) traverses to (2) and is stored (3).

# Analysis

## Data Collection

The following table lists all evidence items collected by Nuix during the course of the investigation. All data and images were collected utilizing industry-standard practices and were securely retained during transit.

| System Name | Data Collected | SHA1 Hash Value |
| --- | --- | --- |
| SERVER1 |  |  |
| SERVER2 |  |  |
| SERVER3 |  |  |
| SERVER4 |  |  |

## Findings

### Initial Findings

Once Nuix was engaged, an investigator travelled to the CLIENT location/remotely gathered evidence from the client location. The investigator noted the following findings within the first 48 hours:

* Finding 1
* Finding 2
* Finding 3

### Memory Analysis

Memory analysis may yield a tremendous amount of information about the system under investigation. The presence of malware, file links, loaded DLL's, network connection information, registry information and character strings may be available from a memory image. Memory analysis was performed using industry-standard tools, the results of this analysis follow:

|  |  |
| --- | --- |
| System Name | Analysis Summary |
| SERVER1 | Memory analysis showed the following |
| EVIDENCE | |
|  | |

### Registry Analysis - Table 1

The Windows registry is " a database in Windows that contains important information about system hardware, installed programs and settings, and profiles of each of the user accounts on your computer. Windows continually refers to the information in the registry." (Microsoft)

|  |  |  |
| --- | --- | --- |
| System Name | Registry Hive | Summary |
| Server1 | HKLM/SAM  HKLM/Security  HKLM/Software  HKLM/System  NTUSER/\*username\* | The Security Account Manager (SAM) is a database present on Windows systems that stores user accounts and security descriptors for users on the local computer. (Microsoft, Technet)  The Security hive contains security audit settings.  The Software registry hive contains information related to software installed on a Windows system. Examples are software version, install dates, application paths and startup configuration.  The System registry hive contains settings and configuration data related to system devices and settings. Examples include: network settings, service entries, hostname, physical devices and remote connectivity.  The NTUser hive is a hive that stores personal configuration settings for each unique user. It stores information about recent access, application use, items that were searched for and many other items. |
| EVIDENCE | | |
|  | | |

### Registry Analysis - Table 2

|  |  |  |
| --- | --- | --- |
| System Name | Registry Hive | Summary |
| Server1 | HKLM/SAM  HKLM/Security  HKLM/Software  HKLM/System  NTUSER/\*username\* | The Security Account Manager (SAM) is a database present on Windows systems that stores user accounts and security descriptors for users on the local computer. (Microsoft, Technet)  The Security hive contains security audit settings.  The Software registry hive contains information related to software installed on a Windows system. Examples are software version, install dates, application paths and startup configuration.  The System registry hive contains settings and configuration data related to system devices and settings. Examples include: network settings, service entries, hostname, physical devices and remote connectivity.  The NTUser hive is a hive that stores personal configuration settings for each unique user. It stores information about recent access, application use, items that were searched for and many other items. |
| EVIDENCE | | |
|  | | |

### Log Analysis

Logs are found in various formats depending on Device type, Operating System, software version, etc… Logs were extracted from the systems under review and analyzed for Indicators of Compromise. The following log excerpts contain events and evidence pertinent to the current investigation (some log entries may have been redacted to improve clarity and formatting):

**Windows Event Log - Table 1**

|  |  |
| --- | --- |
| System Name | Analysis Summary |
| SERVER1 | Log analysis showed the following |
| EVIDENCE | |
|  | |

**Windows Event Log - Table 2**

|  |  |
| --- | --- |
| System Name | Analysis Summary |
| SERVER1 | Log analysis showed the following |
| EVIDENCE | |
|  | |

**Web Log - Table 1**

|  |  |
| --- | --- |
| System Name | Analysis Summary |
| SERVER1 | Log analysis showed the following |
| EVIDENCE | |
| **Sample screenshot below** | |

**Web Log - Table 2**

|  |  |
| --- | --- |
| System Name | Analysis Summary |
| SERVER1 | Log analysis showed the following |
| EVIDENCE | |
| **Sample screenshot below** | |

**Generic Log - Table 1**

|  |  |
| --- | --- |
| System Name | Analysis Summary |
| SERVER1 | Log analysis showed the following |
| EVIDENCE | |
|  | |

### Timeline Analysis

Timeline analysis is the process of ordering events during an incident by their recorded timestamps. Some items, like files, carry multiple timestamps for access, change, creation and modification while others carry only a single timestamp like last modification.

A timeline of events on the systems under investigation was produced and analyzed for Indicators of Compromise. The results of this analysis are shown below.

|  |  |
| --- | --- |
| System Name | Analysis Summary |
| SERVER1 | Log analysis showed the following |
| EVIDENCE | |
|  | |

### Database Analysis

Databases were extracted and analyzed during the course of the investigation.

|  |  |
| --- | --- |
| System Name | Analysis Summary |
| SERVER1 | Database analysis showed the following |
| EVIDENCE | |
|  | |

### Malware Analysis

### Attack Origination

Nuix discovered the following information with regards to the source and destination of the attack(s).

|  |  |  |
| --- | --- | --- |
| IP Address | Origin COuntry | Summary |
| 192.168.1.1 | USA-Montana | Source IP of system used to scan Website |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Deficiencies

While this list is comprehensive, it may not list specific deficiencies related to regulatory or compliance issues particular to the CLIENT's business. Rather, this list reflects specific deficiencies noted by Nuix during the investigation.

During the course of the investigation Nuix discovered the following security deficiencies:

1. **Network**

**\*\*\*\*\*Delete deficiencies that are not applicable\*\*\*\*\***

1. Critical data and systems reside on the same network as User desktops and resources. (no network segmentation)
2. Firewalls were not properly configured for ingress filtering (unused or vulnerable services were available to the internet)
3. Firewalls were not properly configured for egress filtering (unused or vulnerable services were available outbound from the network)
4. Remote access services were available to the internet without strong access control (two-factor auth, VPN)
5. Critical systems or systems storing sensitive data had full access to "surf" the web
6. Unsecured wireless networks were available
7. **System**
8. Users have Administrator access to local desktops.
9. Operating systems were not patched or updated
10. Antivirus/Antimalware was not in place
11. Antivirus/Antimalware was out of date
12. Malware was present on the systems
13. **Policy and/or Procedural**
14. No Incident Response plan was in place
15. No IT Security Policy was in place
16. Penetration testing was not being performed

.

## Recommendations

### Customer Actions

|  |  |
| --- | --- |
| Computer Systems | Recommendation |
|  | Implement complex password enforcement (at least seven characters, with at least one numeric and one special) |
| Rotate passwords at least every 90 days and set policy to prevent password re-use |
| If malware was present, Nuix recommends a full system wipe and rebuild |
| Deploy and monitor a centrally-managed Antivirus system to all endpoints, regardless of OS |
| Deploy and monitor file integrity monitoring software |
| Remove local administrator privileges for users on Windows workstations |
| Require two-factor access for any and all remote access services |
| Require unique user id's for all personnel in all roles |
| Maintain a patch cycle for all systems that ensures critical patches are installed in a timely manner |
| Encrypt or remove sensitive data at rest. If encryption is used, ensure that crypto keys are not available on the same network as the encrypted data. (use physical access to protect crypto keys) |
| Remove unnecessary services, applications and network protocols |
| Remove or disable unneeded default accounts |
|  | Configure account lockout policy to limit brute force attempts |
|  |  |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
| Network Systems | Recommendation |
|  | Segment systems with valuable or critical data from the main user network and implement strong access controls |
| Implement ingress and egress filtering utilizing firewalls that perform stateful packet inspection |
| Implement Network Access Control (NAC) |
| Implement and monitor and IDS/IPS system |
| Implement Web Application Firewalls (WAF) for any web-serving resources |
| Perform Goal-based Penetration Testing annually or after each major change |
| Maintain a testing environment separate from the production network |
|  |
|  |

|  |  |
| --- | --- |
| IT Policy | Recommendation |
|  | Write and maintain an IT security policy and Incident Response Plan |
| Review and test your IR plan at least annually |
| Conduct annual Security Awareness Training |
| Perform Data Discovery (know where your sensitive data is housed) |
| Implement and maintain an IT Security Amnesty Policy (to insure your employees know they will not be terminated for reporting a security incident) |
| Retain all system and networking logs for a minimum of 90 days (readily accessible) and one year (archived) |
| Create, document and implement a patching process |
|  |
|  |
|  |

# Appendix

## Report Contacts

|  |  |  |
| --- | --- | --- |
| CLIENT COntact | Email | Phone |
|  |  |  |
|  |  |  |
| INVESTIGATOR CONTACT | Email | Phone |
|  |  |  |
|  |  |  |

BIBLIOGRAPHY

Microsoft. (n.d.). *Technet*. Retrieved November 3, 2014, from technet.microsoft.com: http://technet.microsoft.com/en-us/library/cc756748%28v=ws.10%29.aspx

Microsoft. (n.d.). *What is the registry?* Retrieved November 3, 2014, from Windows.Microsoft.com: http://windows.microsoft.com/en-US/windows-vista/What-is-the-registry