**Name of Organization**

**Incident Report**

December 2021

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number | Revision Date | Summary of Changes Made | Changed By |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Instructions

The (Name of Organization) Incident Response Forensic Report is designated For Official Use Only (FOUO) and is the property of (Name of Organization). Only (Name of Organization) representatives may distribute this document to individuals on a need-to-know basis. Distribution by other individuals without prior authorization is prohibited. This document is unclassified but contains sensitive information.

**Table of Contents**

[I. Executive Summary 7](#_Toc88643951)

[II. Corrective Actions 7](#_Toc88643952)

[III. Recommendations 7](#_Toc88643953)

[IV. Timeline of Actions 8](#_Toc88643954)

[V. List of Recipients 8](#_Toc88643955)

[VI. Initial Incident Discovery 9](#_Toc88643956)

[Summary 9](#_Toc88643957)

[Incident Action Plan 9](#_Toc88643958)

[Description of system(s) in question 10](#_Toc88643959)

[Identified Computer System(s) 10](#_Toc88643960)

[Security Mechanisms 10](#_Toc88643961)

[Initial Forensic Discovery 10](#_Toc88643962)

[Initial Corrective Action 11](#_Toc88643963)

[Participants 11](#_Toc88643964)

[VII. Forensic Process 11](#_Toc88643965)

[Device/Data Information 12](#_Toc88643966)

[Acquired media description – Drive image #1 12](#_Toc88643967)

[Forensic Analysis – Memory 13](#_Toc88643968)

[Forensic tools used & versions 13](#_Toc88643969)

[Identification of the image 13](#_Toc88643970)

[Identification of suspicious processes 14](#_Toc88643971)

[Identification of Suspicious Connections 14](#_Toc88643972)

[Open files 15](#_Toc88643973)

[Malicious URLs 15](#_Toc88643974)

[Driver Listing and Order 16](#_Toc88643975)

[Callbacks 16](#_Toc88643976)

[Mutex scan 16](#_Toc88643977)

[Detection of hidden/injected code or DLLs in memory 17](#_Toc88643978)

[Malware Hooks 17](#_Toc88643979)

[Threads 18](#_Toc88643980)

[String Search 18](#_Toc88643981)

[Forensic Analysis – Packet capture 18](#_Toc88643982)

[Forensic Analysis – Proxy Logs 18](#_Toc88643983)

[Forensic Analysis - Master File Table 19](#_Toc88643984)

[Forensic Analysis - Firewall Logs 19](#_Toc88643985)

[Forensic Analysis – SIEM Alerts 19](#_Toc88643986)

[Forensics Analysis – Web/Proxy/SQL Logs 19](#_Toc88643987)

[Forensic Analysis - Malicious Files 20](#_Toc88643988)

[Filename #1 20](#_Toc88643989)

[Filename #2 21](#_Toc88643990)

[IP/Domain Lookup 22](#_Toc88643991)

[domainName1.com 22](#_Toc88643992)

[domainName2.com 22](#_Toc88643993)

**Document History**

**INCIDENT COMMANDER** :

**document number :**

**version :**

**status :**

**source :**

**document date :**

**number of pages :**

 **owner :**

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number | Revision Date | Summary of Changes Made | Changed By |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Executive Summary

<Provide a high-level overview of what has occurred>

# Corrective Actions

<Sum up what did you do to correct the problem>

# Recommendations

The strategic recommendations below are based on how the organization views and approaches security from a People, Process, and Technology (PPT) standpoint. The Incident Response team recommends that the organization considers addressing the following strategic areas.

| People |
| --- |
| Risk Level | Risk Summary | Detail |
| High Risk |  |  |
| Medium Risk |  |  |
| Low Risk |  |  |
| Process |
| High Risk |  |  |
| Medium Risk |  |  |
| Low Risk |  |  |
| Technology |
| High Risk |  |  |
| Medium Risk |  |  |
| Low Risk |  |  |

The strategic recommendations above are classified based on their priority. The table below summarizes the strategic recommendation priority criteria used.

| Strategic Recommendation Priority Criteria |
| --- |
| High Risk | High priority recommendations should be considered top priority. Resolution should be started immediately with a goal of resolving them within the next three months. |
| Medium Risk | Medium priority recommendations should be considered for implementation once high priority items are underway or completed. Resolution should be obtained within the next three to six months. |
| Low Risk | Low priority recommendations should not be considered for implementation until all high and medium priority items are completed or underway. Resolution should be obtained within the next year. |

# Timeline of Actions

Below is the timeline of actions regarding the incident. This has been shortened for brevity.

| Date | Time | User | IP | Notes |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# List of Recipients

This report is internal confidential; any part shouldn’t be disclosed without a written statement from the Incident Commander.

| Name | Role | Email |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

# Initial Incident Discovery

## Summary

<Summarize the initial discover process and what has been discovered>

|  |  |
| --- | --- |
| Incident ticket number |  |
| Brief Description:(Of the Incident and its resolution) |  |
| Description of Customer Impact:(How did the Incident(s) affect the Customer’s business)  |  |
| Affected Service(s) / Application(s): |  |
| Contract Group / Number: optional |  |
| Service / Application Owner: |  |
| Affected Department(s): optional |  |
| Affected Location(s): optional |  |
| Affected number of Users: |  |
| Start Date / Time of incident: |  |
| End Date / Time of incident: |  |
| Duration time incident during service hours: |  |
| Service Level/Violation: optional |  |

## Incident Action Plan

<List items that need/needed to be done and who’s assigned to the tasks – SMART deliverables>

| # | Action Statement(Produce effect by taking action) | Action Deliverable(Mandatory to review output of action before action closure) | Action Category | Action Priority | Action Owner(Name Team and Person) | Target Date(dd.mm.yyyy) | Completion Date(dd.mm.yyyy) |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 |  |  | Choose an item. | Choose an item. |  | Click here to enter a date. | Click here to enter a date. |
| 2 |  |  | Choose an item. | Choose an item. |  | Click here to enter a date. | Click here to enter a date. |
| 3 |  |  | Choose an item. | Choose an item. |  | Click here to enter a date. | Click here to enter a date. |
| 4 |  |  | Choose an item. | Choose an item. |  | Click here to enter a date. | Click here to enter a date. |
| 5 |  |  | Choose an item. | Choose an item. |  | Click here to enter a date. | Click here to enter a date. |
| 6 |  |  | Choose an item. | Choose an item. |  | Click here to enter a date. | Click here to enter a date. |
| 7 |  |  | Choose an item. | Choose an item. |  | Click here to enter a date. | Click here to enter a date. |
| 8 |  |  | Choose an item. | Choose an item. |  | Click here to enter a date. | Click here to enter a date. |

##

## Description of system(s) in question

<What business functions do the system(s) provide? What datacenter/cloud provider are they hosted in? What network do they reside on? What other systems or data do these systems have access to?>

##

## Identified Computer System(s)

<Describe the systems in full technical detail>

##

## Security Mechanisms

<Are there any security mechanisms in place that pertain to this system? Like firewalls, IDS, IPS, access control lists, etc.>

##

## Initial Forensic Discovery

<During the initial discovery phase what was found? Port Scans, modified systems files, erroneous network traffic, etc.>

## Initial Corrective Action

<Before you can fully investigate the problem what are you going to do temporarily to avoid risk and perform the analysis? Examples: the system is disconnected from the network, apps have been transferred to another system, etc.>

## Participants

| Name | Role | Email | Phone |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Forensic Process

<Provide the steps used to perform the investigation. This section will vary according to the type of investigation. Add or delete sections as needed>

To investigate the malware infection, the following artifacts were analyzed:

| Artefact | Tool Used  | Goal |
| --- | --- | --- |
| Memory Dumps |  | Determine the extent of infection on a machine. A memory capture can assist in finding rootkits, malicious modules, hidden processes, and connections. |
| Packet Captures (PCAP) |  | Determine the network activity occurring on a machine while infected and provide clues as to the malware’s behavior as well as additional infected machines on the network |
| Proxy Logs |  | Determine if the new extra signatures provided by the organization were eradicating the malware. The malware beaconed out to specific domains, and these were searched upon on a daily basis. |
| Master File Table (MFT) |  | With any NTFS filesystem, the MFT must be used when a new file is created on the machine. Although it is not necessarily updated when a file is modified or accessed, there will be an MFT entry for almost every file installed on a machine. Even if a file is deleted, there is a chance its MFT entry is still intact.  |
| Firewall Logs |  |  |
| Sentinel Alerts |  | Used in the detection of incidents and to determine if containment and eradication strategies have resolved the incident.  |
| Web/SQL Logs |  | Used for detection of website defacements, Denial of Service attacks, data leakage, etc. |
| Malicious Files |  |  |
| Other |  |  |

##

## Device/Data Information

<This should be completed for every drive analyzed/memory dump acquired>

## Acquired media description – Drive image #1

| Computer Workstation |
| --- |
| Hostname |  |
| Memory Dump Filename |  |
| Size |  |
| SHA1 Hash |  |
| MD5 Hash |  |
| Format |  |
| Date acquired |  |
| Acquisition tool & version |  |
| Installed OS & version |  |
| Configured time zone |  |
| Configured network settings | Type | <DHCP/static> |
| IP |  |
| Netmask |  |
| Gateway |  |
| DNS1 |  |
| DNS2 |  |
| domainname |  |
| DHCP server address |  |
| <other> |  |

## Forensic Analysis – Memory

<Each artifact listed in the ‘forensic approach’ gets its own section. Of course, these can be added/removed as necessary per case. Any additions should be maintained in the master copy>

## Forensic tools used & versions

| Tool name | Version |
| --- | --- |
| Volatility |  |
| HBGary Responder |  |
| Auditviewer |  |
| Memoryze |  |
| Bulk\_Extractor |  |

## Identification of the image

<This step is used to identify the operating system, service pack, and hardware architecture (32 or 64 bit), but it also contains other useful information such as the time the sample was collected.>

*<Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)*

*AS Layer1 : JKIA32PagedMemoryPae (Kernel AS)*

*AS Layer2 : FileAddressSpace*

*PAE type : PAE*

*DTB : 0x33e000L*

*KDBG : 0x8054d2e0L*

*Number of Processors : 2*

*Image Type (Service Pack) : 3*

*KPCR for CPU 0 : 0xffdff000L*

*KPCR for CPU 1 : 0xba338000L*

*KUSER\_SHARED\_DATA : 0xffdf0000L*

*Image date and time : 2013-06-15 11:42:20 UTC+0000*

*Image local date and time : 2013-06-15 11:42:20 +0000>*

## Identification of suspicious processes

The next step in the investigation is to identify if (hidden) suspicious processes are running on the system.

<List the processes deemed suspicious and why>

| Offset(V) | Name | PID | PPID | Start Time (UTC) |
| --- | --- | --- | --- | --- |
| 0x89f47020 | svchost.exe | 756 | 580 | 2012-11-09 14:05:30 |
| 0x88d1a020 | iexplore.exe | 5832 | 756 | 2012-11-09 15:39:35 |
| 0x890edba0 | iexplore.exe | 3684 | 5832 | 2012-11-09 15:39:35 |
|  | iexplore.exe | 4464 | 5832 | 2012-11-09 16:04:03 |

## Identification of Suspicious Connections

Most malware samples connect to malicious systems hosted under publicly accessible domains. These domains can be used for various purposes: downloading other malware samples; receiving commands from a “bot-herder”; receiving updated configuration files. By finding ‘\_TCPT\_OBJECT’ structures using pool tag scanning, artefacts from previous connections (that have since been terminated) can be discovered in addition to the active ones. Below a small sample of the discovered connections using the linked lists:

<volatility connscan, connections, sockscan, sockets>

| Offset(V) | Local Address | Remote Address | PID |
| --- | --- | --- | --- |
|  |  |  |   |
|  |  |  |   |
|  |  |  |   |

However, malware can sometimes hide itself from the lists, therefore a Volatility plugin called connscan should be run to search for these processes.

| Offset | Local Address | Remote Address | PID |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Open files

<iehistory plugin for Volatility, bulk\_extractor, HBGary>

A list of open files during the memory extraction should be investigated for anomalies and suspicious files. Look for link files, which could potentially have been infected being accessed by the machine at the point of acquisition.

A Volatility plugin called ‘filescan’ can be run to determine open files during the point of acquisition. This could be used to help determine any files the malware was using or were potentially infected.

<Be sure to explain why you are showing these>

| Offset (V) | Type | Name |
| --- | --- | --- |
| 0x08eb89c8 | 0x8a54dad0 | \\Documents and Settings\\...\\Application Data\\Microsoft\\Office\\Recent\\G8.LNK |
| 0x09575570 | 0x8a54dad0 | \\Documents and Settings\\... \\Recent\\G8.lnk |
| 0x09581268 | 0x8a54dad0 | \\Documents and Settings\\...\\Recent\\11 November.lnk |
| 0x0a405110 | 0x8a54dad0 | \\Documents and Settings\\...\\Start Menu\\Programs\\Internet Explorer.lnk\x00s\\desktop.ini\x00F5E7DA5}\\0000\x00sion\\Internet Setting |
| 0x0a470a68 | 0x8a54dad0 | \\Documents and Settings\\...\\Application Data\\Microsoft\\Office\\Recent\\11 November.LNK |

LNK files are of interest as the malware can spread by hiding the file and displaying a link file which executes the malware on the machine as well as displaying the file.

## Malicious URLs

A list of URLs should be extracted from the acquired memory dump. Export and compare against a Threat Intelligence database for known malicious websites/URLs. Note URLS of interest below:

* URL1
* URL2

<explain why those URLs are of interest>

##

## Driver Listing and Order

Windows uses a layered driver architecture, or “driver chain” so that multiple drivers can inspect or respond to an Input/Output Request Packet (IRP). Rootkits often insert drivers (or devices) into this chain for filtering purposes (to hide files, hide network connections, steal keystrokes or mouse movements). The devicetree plugin in Volatility shows the relationship of a driver object to its devices.

## Callbacks

<Volatility ‘callbacks’ plugin>

| Type | Callback | Owner |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

## Mutex scan

A Mutex helps to serialize access to a resource. Some applications employ a Mutex to ensure that only a single instance is running. A mutex is a concept that is widely used in concurrent programming, but also used by malware for example to ensure not to infect the same machine twice.

volatility mutantscan –f [filename of memory-dump]

This command gives a full list that contains a lot of nameless mutants. Therefore, it’s recommended to apply the -s or --silent switch, which cuts the list down to named mutants.

The output can be matched against known Mutex names for the type of malware in case a sample is available of the malware. Example:

| Offset(P) | #Ptr | #Hnd | Thread | CID | Name | Malware |
| --- | --- | --- | --- | --- | --- | --- |
| 0x09139bc0 | 2 | 1 | 0x00000000 |  | MSCTF.Shared.MUTEX.EPN | YES |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

## Detection of hidden/injected code or DLLs in memory

Volatility’s ‘malfind’, ‘dlllist’ and ‘procexec’ plugins can be used. Output of malfind matched against VirusTotal database>:

## Malware Hooks

Malware can hook user and system calls to hide themselves from an analyst. They do this by hooking certain calls. Volatility has two plugins, ‘apihooks’ and ‘ssdt’ to look for suspicious modules hooking into processes and kernel calls. Apihooks find Import Address Table (IAT), Export Address Table (EAT), Inline style hooks, as well as several special types of hooks.

<plugin Apihooks in Volatility>

| Name | Type | Target | Value |
| --- | --- | --- | --- |
| Svchost.exe[880] | Inline | Kernel32.dll!0x50 | 0x7c801a28 JMP 0x50d0fef |
|  |  |  |  |
|  |  |  |  |

The SQL Server Data Tools (SSDT) plugin scans for ETHREAD objects and searches for a pointer within each ETHREAD and displays its location and owner. This can detect rootkits make copies of SSDTs and then assign them to a specific thread.

<plugin ssdt in volatility>

| Entry Number | Location | Table Entry |
| --- | --- | --- |
| 0x0000 | 0x805a4638 | (NtAcceptConnectPort) owned by ntoskrnl.exe |
|  |  |  |
|  |  |  |

## Threads

Threads plugin for volatility; filter using suspicious process (-p) or filter with -F (use -L to list filters)

## String Search

Try using ‘grep’ against the dlldump, malfind, and vaddump output

## Forensic Analysis – Packet capture

Depending on the type of case this section will vary… It can be used for exfil, malware, unauthorized access/login, website defacement, etc. export the TCP conversations from Wireshark.

<Insert .cap or .pcap here>

| Source IP | Destination IP | Port | Sum of Bytes | Sum of Bytes src ⇨ dst | Sum of Bytes dst ⇨ src |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Those services are mainly concerned:

| Port | Service |
| --- | --- |
|  |  |
|  |  |
|  |  |

Port list by IANA:

http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

##

## Forensic Analysis – Proxy Logs

This section is useful in dealing with malware or unauthorized usage incidents. It can also be used to determine if mitigation strategies were successful.

Example: These domains were searched for across all days. All were observed over TCP port 443.

| Date | Domain | Successful? | First observed | Last Observed | # connections |
| --- | --- | --- | --- | --- | --- |
|  | suspDomainA | Yes | 01.01.2012 12:00 CET | 01.01.2012 12:00 CET | 8 |
|  | suspDomainB | No | 01.01.201212:00 CET | 01.01.201212:00 CET | 16 |
|  | suspDomainC | No | 01.01.201212:00 CET | 01.01.201212:00 CET | 32 |

## Forensic Analysis - Master File Table

Use ‘MFTDUmp’ to help determine infection point, verify infection, dropped files, program run, etc.

If a file is created on a machine, an entry must be placed in the MFT. Even if a file is deleted its presence may still be present in the MFT if it is not overwritten.

##

## Forensic Analysis - Firewall Logs

If firewall logs can be used to show the attempts made (successful or not) to infiltrate/exfiltrate the network, they should be listed here.

##

## Forensic Analysis – SIEM Alerts

These can show the initial detection mechanisms for an incident as well as showing the effectiveness of containment/eradication strategies.

Any additional rules created to aid in the incident should be noted here.

##

## Forensics Analysis – Web/Proxy/SQL Logs

Describe what you have found in web/proxy/sql logs.

##

## Forensic Analysis - Malicious Files

## Filename #1

| Information |
| --- |
| Detection name: |  |
| Location: |  |
| Created: |  |
| MD5 Hash: |  |
| SHA1 Hash: |  |
| Size: |  |
| <Any other information> |  |

* General activity

<List any activities here>

* File operations

<List any file activities here>

* Service activity

<List any services here>

* Registry activity

<list any registry activity here>

* Network activity

<list any network activity here>

* AV vendor escalation

e.g., Suspicious file was sent to <vendor name>, ticket number was <xxx>

<vendor name> identified threat <threat name>. Signature version <xxx> was created to deal with this threat.

## Filename #2

| Information |
| --- |
| Detection name: |  |
| Location: |  |
| Created: |  |
| MD5 Hash: |  |
| SHA1 Hash: |  |
| Size: |  |
| <Any other information> |  |

* General activity

<List any activities here>

* File operations

<List any file activities here>

* Service activity

<List any services here>

* Registry activity

<list any registry activity here>

* Network activity

<list any network activity here>

* AV vendor escalation

e.g., Suspicious file was sent to <vendor name>, ticket number was <xxx>

<vendor name> identified threat <threat name>. Signature version <xxx> was created to deal with this threat.

# IP/Domain Lookup

## domainName1.com

| General information |
| --- |
| Domain name |  |
| IP address |  |
| Location |  |
| Registrar | [RIPE/ARIN/APNIC/AFRINIC/LACNIC] |
| Registered to |  |
| Blacklisted |  |

| Site integrity |
| --- |
| Threat expert |  |
| Google |  |
| URL Query |  |
| <any other> |  |

## domainName2.com

| General information |
| --- |
| Domain name |  |
| IP address |  |
| Location |  |
| Registrar | [RIPE/ARIN/APNIC/AFRINIC/LACNIC] |
| Registered to |  |
| Blacklisted |  |

| Site integrity |
| --- |
| Threat expert |  |
| Google |  |
| URL Query |  |
| <any other> |  |

Appendix A Administrative Contacts

| Name | Title | Email | Phone Numbers |
| --- | --- | --- | --- |
| The organization |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| <Customer> |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Appendix B Evidence Receipt/Forensic Form

Appendix C Extracted files

<attach or list all files found in pcap files>