**Internal Memorandum**



**To: Regner Sabillon, CISO**

**From: Ahmed Almass and Mike Carlson**

**RE: Weekly Report 5 – Malware Lab**

**2018-11-26**

In this week, we’ve selected a malware sample. The sample we’ve selected was Dyre also known as Dyreza. The reason why we chose this malware is that it works on our specific operating system, Windows 7 64bit. Also, this family of malware is still being used. The current version is designated Trickbot. More info may be found at:

https://jask.com/trickbot/

On the Kali linux virtual machine, we will be able to access the internet and upload the malware from Github at the following URL:

https://github.com/ytisf/theZoo/tree/master/malwares/Binaries/Dyre?fbclid=IwAR0QdvUBWFi-JPnHoHSxdQSyIwR8pDe-hrSUJvJNzkV\_c0gSjtIcn6eOYXo

Next week we will transport it to the Windows 7 victim machine. When initially uploaded the Malware is zipped with a password. For security measures there will be a firewall in after Kali end and there be no internet access on the windows 7 end. The malware only works on the Windows 7 Operating system, so it will not work on the Kali Linux end. Many of the other groups appear to have concentrated on ransom ware and backing Trojan represents something that is a significant class of malware.

The project is still basically on track, further to our schedule below. The main objective for the week was malware selection, which is complete. The virtual machine continues to operate. The firewall has not yet been included yet. However, the isolation switches have just arrived today. Next week the major objective is basis analysis guidelines.

|  |  |  |
| --- | --- | --- |
| **School Fall Term Week:** | **Objective:** | **Submission Date:** |
| Week 8, Oct 22-28 | Report 1: Project proposal (3%) | Oct 29 |
| Week 9, Oct 29-Nov 4 | Report 2: Network configuration and diagrams (2%) | Nov 5 |
| Week 10, Nov 5-Nov 11 | Report 3: Machine configuration and diagrams (1%) | Nov 12 |
| Week 11, Nov 12-Nov 18 | Report 4: Tools for the virtual lab (1%) | Nov 19 |
| Week 12, Nov 19-Nov 25 | Weekly report 5: Malware sample selection and justification (1%) | Nov 26 |
| Week 13, Nov 26-Dec 2 | Weekly report 6: Basic analysis guidelines (1%) | Dec 3 |
| Week 14, Dec 3-Dec 9 | Weekly report 7: Advanced analysis guidelines (1%) | Dec 9 |
| Week 15, Dec 10-14 | Delivery of final project report (15%),  Project presentation + demo (10%) and Project assessment (20%) | Dec 1 |

The Agile project development backlog list has been updated as attached below: During the last week Mike Carlson was away sick – so the work this week was one by Ahmed Almass.

Ahmed Almass Malware analyst Mike Carlson Manager Malware analyst

Email address: ahmed.almass@edu.sait.ca Email address: mike.carlson@edu.sait.ca

Phone number (403) 667 1234 Phone number (403) 399 7151

|  |  |
| --- | --- |
| **Malware Project - November 4th, 2018 – Backlog List** |  |
|  |  |
| **Agile Development** |  |
| Backlog List / Proposal | objectives |
| Backlog List Oct 22-28 | Done |
| Backlog List Oct 29-Nov 4 | Done |
| Backlog List Nov 5-Nov 11 | Done |
| Backlog List Nov 12-Nov 18 | Done |
| Backlog List Nov 19-Nov 25 | Done |
| Backlog List Nov 26-Dec 2 | x |
| Backlog List Dec 3-Dec 9 | x |
| Backlog List Dec 10-14 | x |
|  |  |
|  |  |
| **Admin Functions** |  |
| Weekly Report / Proposal | complete |
| Weekly Report Oct 22-28 | Done |
| Weekly Report Oct 29-Nov 4 | Done |
| Weekly Report Nov 5-Nov 11 | Done |
| Weekly Report Nov 12-Nov 18 | Done |
| Weekly Report Nov 19-Nov 25 | Done |
| Weekly Report Nov 26-Dec 2 | x |
| Weekly Report Dec 3-Dec 9 | x |
| Weekly Report Dec 10-14 | x |
|  |  |
|  |  |
| **Original Project Objectives** |  |
| Pick 2 malware samples | Done |
| Final report | started |
| A Virtual network | version 1 |
| Virtual Machine # 1 for launching malware attacks | version 1 |
| Virtual Machine # 2 for launching malware attacks | version 1 |
| Virtual Machine for static analysis (Kali Machine) | x |
| Virtual Sniffer machine | version 1 |
| Antivirus/Antimalware tools | x |
|  |  |
| **Added Project Objectives** |  |
| Anti VM sensor implementation | x |
| Analysis tools | started |
| Gant Chart | preliminary |
|  |  |
| **Analysis Tools:** |  |
| ApateDNS v1.0 | on Win 7 vm |
| Autoruns v13.51 | on Win 7 vm |
| Process Explorer V16.1 | on Win 7 vm |
| Process Monitor V3.20 (ProcMon) | on Win 7 vm |
| CaptureBAT V2.0.0-5574 | on Win 7 vm |
| CFF Explorer x86 | on Win 7 vm |
| Dependency Walker v2.2.6000 | on Win 7 vm |
| Exeinfo PE v0.0.4.2 | on Win 7 vm |
| FileAlyzer V2.0.5.57 | on Win 7 vm |
| McAfee FileInsight V2.1 Hex Editor | on Win 7 vm |
| Hex Editor Neo V6.20 Hex Editor | on Win 7 vm |
| IDA Pro Free V5.0 | on Win 7 vm |
| Md5deep - Windows | on Win 7 vm |
| OllyDbg V1.10 - 32-bit | on Win 7 vm |
| OfficeMalScanner V0.54 | on Win 7 vm |
| OleDump | on Win 7 vm |
| Peid V0.95 | on Win 7 vm |
| Pestudio 8.54 | on Win 7 vm |
| PEView V0.9.9.0 | on Win 7 vm |
| Regshot V1.9.0 x86 | on Win 7 vm |
| Rekall V1.5.2 Furka x86 | on Win 7 vm |
| Resource Hacker V4.2.5 | on Win 7 vm |
| Mandiant Memoryze V3.0 | on Win 7 vm |
| Upx V3.91 - Packer | on Win 7 vm |
| WinDbg V6.11.1.404 - Windows Debugger | on Win 7 vm |
| Wireshark Win32 V1.10.1 | on Win 7 vm |
| Burp Suite Pro | on Win 7 vm |
| iNetsim | on Win 7 vm |