
**ID:** 467975
**Sample Name:** nitdmexcel_18-0-1.exe
**Cookbook:** default.jbs
**Time:** 08:29:53
**Date:** 19/08/2021
**Version:** 33.0.0 White Diamond

# Table of Contents

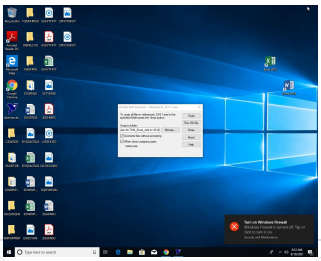
# Windows Analysis Report nitdmexcel_18-0-1.exe

## Overview

### General Information

| | |
|---|---|
| Sample Name: | nitdmexcel_18-0-1.exe |
| Analysis ID: | 467975 |
| MD5: | da499c2a422b15.. |
| SHA1: | 514d01c97416c4.. |
| SHA256: | e3ab996aa8a613.. |
| Infos: | |

Most interesting Screenshot:



### Detection

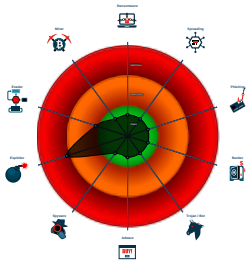

Hidden Macro 4.0

| | |
|---|---|
| Score: | 22 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 80% |

### Signatures

- Yara detected hidden Macro 4.0 in E…
- Uses 32bit PE files
- PE file contains an invalid checksum
- PE file contains strange resources
- PE file contains sections with non-s…

### Classification



## Process Tree

- **System is w10x64**
- nitdmexcel_18-0-1.exe (PID: 3560 cmdline: 'C:\Users\user\Desktop\nitdmexcel_18-0-1.exe' MD5: DA499C2A422B153807FB587D6182EBB6)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Overview

### Initial Sample

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| NI_EX00_fra.mst | JoeSecurity_HiddenMacro | Yara detected hidden Macro 4.0 in Excel | Joe Security | |

## Sigma Overview

**No Sigma rule has matched**

## Jbx Signature Overview

Click to jump to signature section

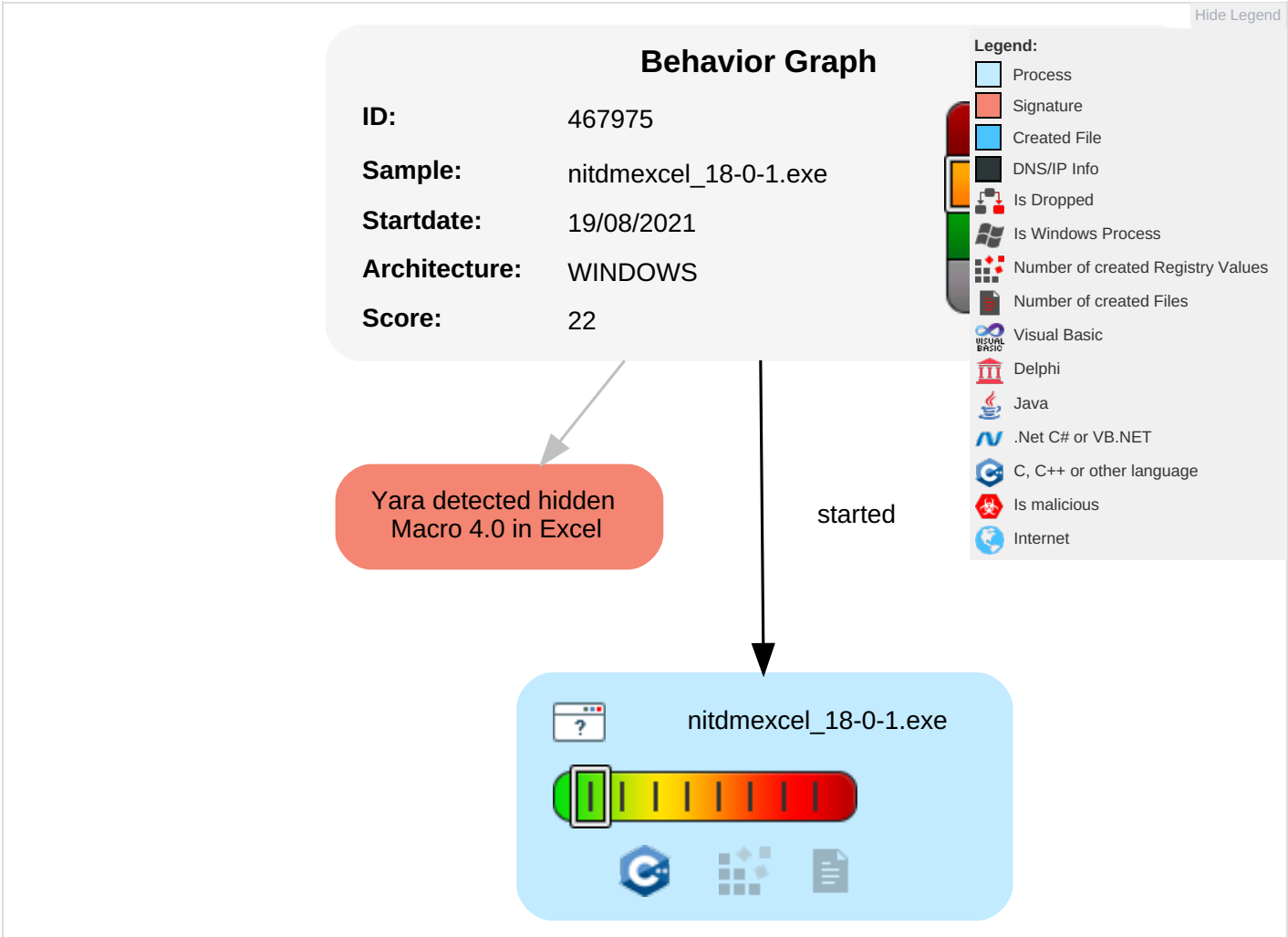
## HIPS / PFW / Operating System Protection Evasion:

**Yara detected hidden Macro 4.0 in Excel**

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Command and Scripting Interpreter 2 | Path Interception | Path Interception | Direct Volume Access | OS Credential Dumping | System Time Discovery 1 | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | Data Obfuscation | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modify System Partition |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Rootkit | LSASS Memory | Security Software Discovery 1 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Junk Data | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | Device Lockout |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Obfuscated Files or Information | Security Account Manager | System Information Discovery 2 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Steganography | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | Delete Device Data |

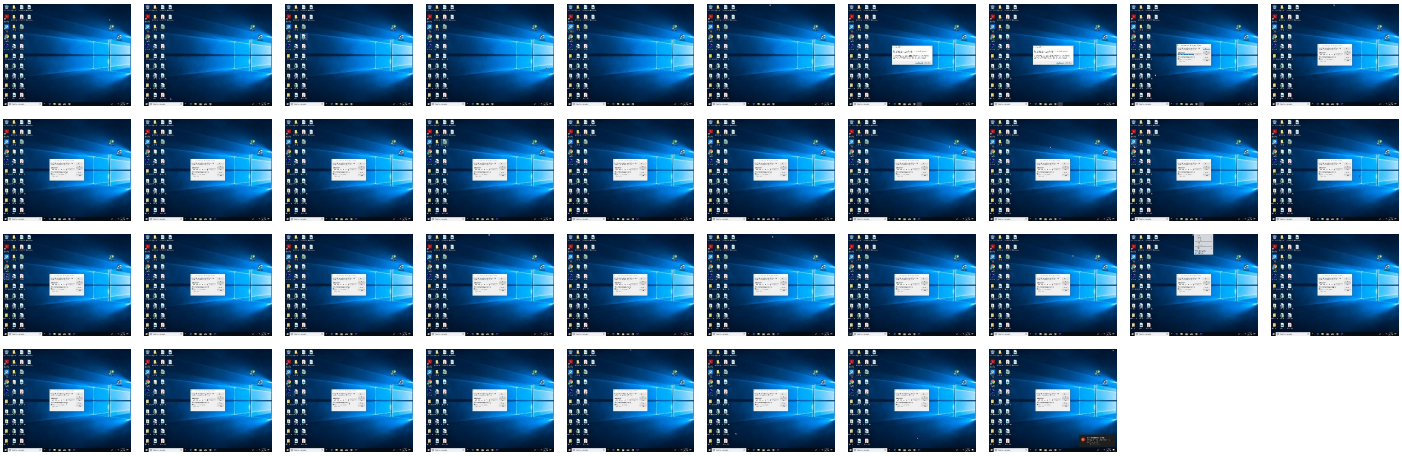
## Behavior Graph




## Screenshots

### Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.




## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| nitdmexcel_18-0-1.exe | 0% | Virustotal | | Browse |
| nitdmexcel_18-0-1.exe | 0% | ReversingLabs | | |

## Dropped Files

**No Antivirus matches**

## Unpacked PE Files

**No Antivirus matches**

## Domains

**No Antivirus matches**

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://ocsp.thawte.com0 | 0% | URL Reputation | safe | |

# Domains and IPs

## Contacted Domains

**No contacted domains info**

## URLs from Memory and Binaries

## Contacted IPs

**No contacted IP infos**

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 467975 |
| Start date: | 19.08.2021 |
| Start time: | 08:29:53 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 6m 22s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | nitdmexcel_18-0-1.exe |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Number of analysed new started processes analysed: | 27 |
| Number of new started drivers analysed: | 0 |
| Number of existing processes analysed: | 0 |
| Number of existing drivers analysed: | 0 |
| Number of injected processes analysed: | 0 |
| Technologies: | • HCA enabled<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | SUS |
| Classification: | sus22.expl.winEXE@1/0@0/0 |
| EGA Information: | Failed |
| HDC Information: | Failed |
| HCA Information: | Failed |

| | |
|---|---|
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .exe |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

**No simulations**

# Joe Sandbox View / Context

## IPs

**No context**

## Domains

**No context**

## ASN

**No context**

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

# Created / dropped Files

**No created / dropped files found**

# Static File Info

### General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386, for MS Windows |
| Entropy (8bit): | 7.9993729480097455 |
| TrID: | • Win32 Executable (generic) a (10002005/4) 99.73%<br>• Winzip Win32 self-extracting archive (generic) (23002/1) 0.23%<br>• Generic Win/DOS Executable (2004/3) 0.02%<br>• DOS Executable Generic (2002/1) 0.02%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | nitdmexcel_18-0-1.exe |
| File size: | 78606216 |
| MD5: | da499c2a422b153807fb587d6182ebb6 |
| SHA1: | 514d01c97416c4dd562a30c430b7e6f7b4e23cc4 |

## General

| | |
|---|---|
| SHA256: | e3ab996aa8a613d02205ccb7fad0141212088974ced8672f332d63a4c2ee8119 |
| SHA512: | e03f698acfd9b2fb97f08b807a1353a577383d0bbe6ebf0ae75dafb333d83f303e4679b538d6539b93f9c195f408ba02a25fe549b793702f4d0dd6e258b34562 |
| SSDEEP: | 1572864:Jotcw0U43/qeP6WR01QSlKe2LCc34RrJ0FVjGyLfnm2rGepGtN4M1DJQmCONvgtD:U9m3ieiWb1e2LCc34MkGfnm2yBSyDJQp |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qw.W5...5...5.....&.....E...5.....8.....4.....4...5...7.....4...Rich5.....PE..L.. |

## File Icon

| | |
|---|---|
| Icon Hash: | 0ac3cc9cd4728e36 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x40a79e |
| Entrypoint Section: | .text |
| Digitally signed: | true |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | 32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED |
| DLL Characteristics: | |
| Time Stamp: | 0x4AEF3FA7 [Mon Nov 2 20:23:03 2009 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | |
| OS Version Major: | 4 |
| OS Version Minor: | 0 |
| File Version Major: | 4 |
| File Version Minor: | 0 |
| Subsystem Version Major: | 4 |
| Subsystem Version Minor: | 0 |
| Import Hash: | f2f9102c7663962c22d17a8dabc5e7ce |

### Authenticode Signature

| | |
|---|---|
| Signature Valid: | **true** |
| Signature Issuer: | CN=VeriSign Class 3 Code Signing 2010 CA, OU=Terms of use at https://www.verisign.com/rpa (c)10, OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US |
| Signature Validation Error: | **The operation completed successfully** |
| Error Number: | 0 |
| Not Before, Not After | • 4/11/2016 5:00:00 PM 7/12/2019 4:59:59 PM |
| Subject Chain | • CN=National Instruments Corporation, O=National Instruments Corporation, L=Austin, S=Texas, C=US |
| Version: | 3 |
| Thumbprint MD5: | 1C8D1A5469552A41DE716974A986D673 |
| Thumbprint SHA-1: | 70B8BA3A50BCDBAD1DC2C86C6DEB1D78215EA111 |
| Thumbprint SHA-256: | 4750C8643DF6099EA03EB3ADA1157EEFC149A3BAC6DBB31760A4DC0AFC41C007 |
| Serial: | 61C3329855F6476CFCB4FCF359E55909 |

### Entrypoint Preview

### Rich Headers

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x11ff5 | 0x12000 | False | 0.624267578125 | data | 6.62017390291 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .rdata | 0x13000 | 0x3742 | 0x4000 | False | 0.329284667969 | data | 4.93791623439 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0x17000 | 0xe744 | 0x2000 | False | 0.17333984375 | data | 1.98004673265 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x26000 | 0x3810 | 0x4000 | False | 0.250915527344 | data | 4.52435452726 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| _winzip_ | 0x2a000 | 0x4ad6000 | 0x4ad6000 | unknown | unknown | unknown | unknown | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

### Resources

### Imports

### Possible Origin

| Language of compilation system | Country where language is spoken | Map |
|---|---|---|
| English | United States |  |

## Network Behavior

**No network behavior found**

## Code Manipulations

## Statistics

## System Behavior

### Analysis Process: nitdmexcel_18-0-1.exe PID: 3560 Parent PID: 1768

### General

| | |
|---|---|
| Start time: | 08:31:09 |
| Start date: | 19/08/2021 |
| Path: | C:\Users\user\Desktop\nitdmexcel_18-0-1.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\nitdmexcel_18-0-1.exe' |
| Imagebase: | 0x400000 |
| File size: | 78606216 bytes |
| MD5 hash: | DA499C2A422B153807FB587D6182EBB6 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | low |

### File Activities

Show Windows behavior

File Read

# Disassembly

## Code Analysis