**MALICIOUS**

Classifications: Ransomware

Threat Names: GoRansom

Verdict Reason: -

| | |
|---|---|
| **Sample Type** | **Windows Exe (x86-64)** |
| **File Name** | **5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe** |
| ID | #7980375 |
| MD5 | 2bbff2111232d73a93cd435300d0a07e |
| SHA1 | b93d633d379052f0a15b0f9c7094829461a86dbb |
| SHA256 | 3160b4308dd9434ebb99e5747ec90d63722a640d329384b1ed536b59352dace6 |
| File Size | 2542.00 KB |
| Report Created | 2023-06-07 02:15 (UTC) |
| Target Environment | win7_64_sp1_en_mso2016 \| exe |

# OVERVIEW

## VMRay Threat Identifiers (20 rules, 147 matches)

| Score | Category | Operation | Count | Classification |
|---|---|---|---|---|
| 5/5 | User Data Modification | Modifies content of user files | 1 | Ransomware |
| | • (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies the content of multiple user files. | | | |
| 5/5 | User Data Modification | Renames user files | 1 | Ransomware |
| | • (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe renames multiple user files. | | | |
| 5/5 | User Data Modification | Modifies Windows automatic backups | 1 | - |
| | • (Process #6) cmd.exe deletes Windows volume shadow copies. | | | |
| 5/5 | User Data Modification | Appends the same extension to many filenames | 1 | Ransomware |
| | • Renames 4486 files by appending the extension ".gdjlosvtnib". | | | |
| 5/5 | YARA | Malicious content matched by YARA rules | 1 | Ransomware |
| | • YARA detected "GoRansom" from ruleset "Ransomware" in memory dump data from (process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe. | | | |
| 4/5 | Reputation | Known malicious file | 1 | - |
| | • The sample itself is a known malicious file. | | | |
| 3/5 | User Data Modification | Possibly drops ransom note files | 1 | Ransomware |
| | • (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe possibly drops ransom note files (creates 510 instances of the file "HOW TO RESTORE YOUR FILES.TXT" in different locations). | | | |
| 2/5 | Anti Analysis | Tries to detect application sandbox | 1 | - |
| | • (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe tries to detect "wine" by calling GetProcAddress() on "wine_get_version". | | | |
| 2/5 | Discovery | Collects information about services | 1 | - |
| | • (Process #3) sc.exe queries information about services via API. | | | |
| 2/5 | Anti Analysis | Delays execution | 1 | - |
| | • (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe has a thread which sleeps more than 5 minutes. | | | |
| 2/5 | Discovery | Searches for sensitive browser data | 1 | - |
| | • (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe searches for sensitive data of web browser "Internet Explorer / Edge" by file. | | | |
| 2/5 | Discovery | Searches for sensitive mail data | 1 | - |
| | • (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe searches for sensitive data of mail application "Windows Mail" by file. | | | |
| 2/5 | Data Collection | Reads sensitive mail data | 1 | - |
| | • (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe tries to read sensitive data of mail application "Windows Mail" by file. | | | |
| 2/5 | Hide Tracks | Hides files | 1 | - |

| Score | Category | Operation | Count | Classification |
|---|---|---|---|---|
| | • (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe hides the file "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Office\Recent\index.dat" by setting its "hidden" attribute. | | | |
| 2/5 | Data Collection | Reads sensitive browser data | 1 | - |
| | • (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file. | | | |
| 1/5 | Hide Tracks | Creates process with hidden window | 4 | - |
| | • (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe starts (process #2) cmd.exe with a hidden window.<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe starts (process #5) cmd.exe with a hidden window.<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe starts (process #6) cmd.exe with a hidden window.<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe starts (process #10) cmd.exe with a hidden window. | | | |
| 1/5 | Defense Evasion | Accesses volumes directly | 26 | - |
| | • (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "D".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "I".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "J".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "K".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "L".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "M".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "E".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "F".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "G".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "H".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "B".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "S".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "T".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "U".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "V".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "W".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "N".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "O".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "P".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "Q".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "R".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "X".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "Y".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "Z".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "C".<br>• (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe opens a handle to directly access the volume "A". | | | |
| 1/5 | System Modification | Modifies application directory | 100 | - |

- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Java\jre1.8.0_171\bin\dtplugin\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Java\jre1.8.0_171\bin\plugin2\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Java\jre1.8.0_171\bin\server\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Java\jre1.8.0_171\bin\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Java\jre1.8.0_171\lib\amd64\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Java\jre1.8.0_171\lib\applet\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Java\jre1.8.0_171\lib\cmm\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Java\jre1.8.0_171\lib\deploy\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Java\jre1.8.0_171\lib\ext\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Java\jre1.8.0_171\lib\fonts\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Java\jre1.8.0_171\lib\images\cursors\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Java\jre1.8.0_171\lib\images\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Java\jre1.8.0_171\lib\jfr\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Java\jre1.8.0_171\lib\management\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Java\jre1.8.0_171\lib\security\policy\limited\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Java\jre1.8.0_171\lib\security\policy\unlimited\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Java\jre1.8.0_171\lib\security\policy\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Java\jre1.8.0_171\lib\security\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Java\jre1.8.0_171\lib\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Java\jre1.8.0_171\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Java\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Microsoft Office\Office16\1033\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Microsoft Office\Office16\OneNote\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Microsoft Office\Office16\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\Microsoft Office\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\WindowsPowerShell\Configuration\Registration\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\WindowsPowerShell\Configuration\Schema\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\WindowsPowerShell\Configuration\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\en\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\WindowsPowerShell\Modules\PackageManagement\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\en-US\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\WindowsPowerShell\Modules\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\WindowsPowerShell\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files (x86)\Microsoft Analysis Services\AS OLEDB\110\Cartridges\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files (x86)\Microsoft Analysis Services\AS OLEDB\110\Resources\1033\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files (x86)\Microsoft Analysis Services\AS OLEDB\110\Resources\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files (x86)\Microsoft Analysis Services\AS OLEDB\110\HOW TO RESTORE YOUR FILES.TXT".
- (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe modifies "C:\Program Files (x86)\Microsoft Analysis Services\AS OLEDB\HOW TO RESTORE YOUR FILES.TXT".

| Score | Category | Operation | Count | Classification |
|---|---|---|---|---|
| 1/5 | Persistence | Installs system startup script or application | 1 | - |
| | • (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe adds "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\HOW TO RESTORE YOUR FILES.TXT" to Windows startup folder. | | | |
| 1/5 | Obfuscation | Resolves API functions dynamically | 1 | - |
| | • (Process #1) 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe resolves 75 API functions by name. | | | |

### Mitre ATT&CK Matrix

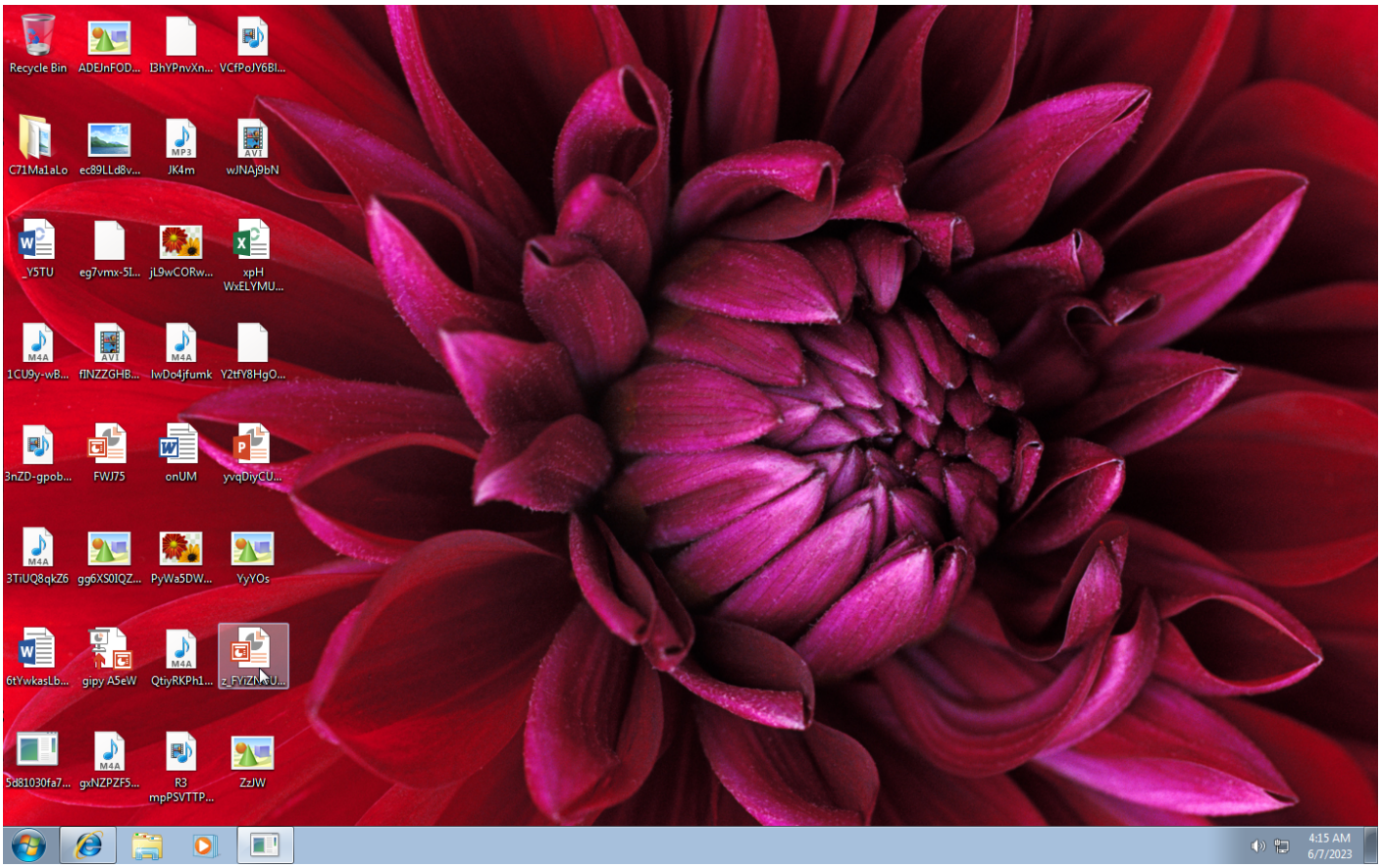
| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | #T1060 Registry Run Keys / Startup Folder | | #T1497 Virtualization/ Sandbox Evasion | #T1081 Credentials in Files | #T1497 Virtualization/ Sandbox Evasion | | #T1119 Automated Collection | | | #T1486 Data Encrypted for Impact |
| | | #T1158 Hidden Files and Directories | | #T1143 Hidden Window | | #T1007 System Service Discovery | | #T1005 Data from Local System | | | #T1490 Inhibit System Recovery |
| | | | | #T1006 File System Logical Offsets | | #T1083 File and Directory Discovery | | | | | |
| | | | | #T1158 Hidden Files and Directories | | | | | | | |
| | | | | #T1045 Software Packing | | | | | | | |

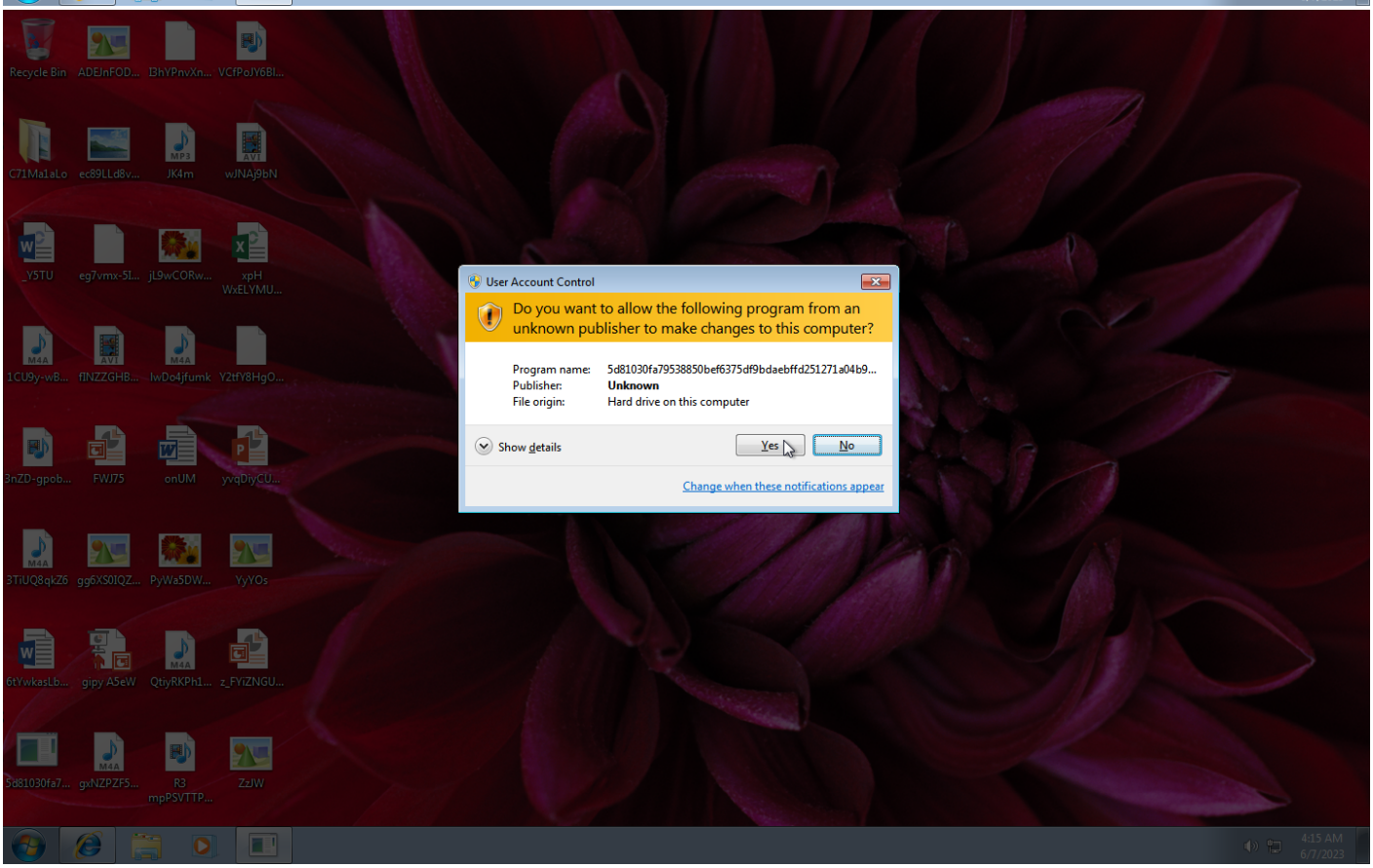
## Sample Information

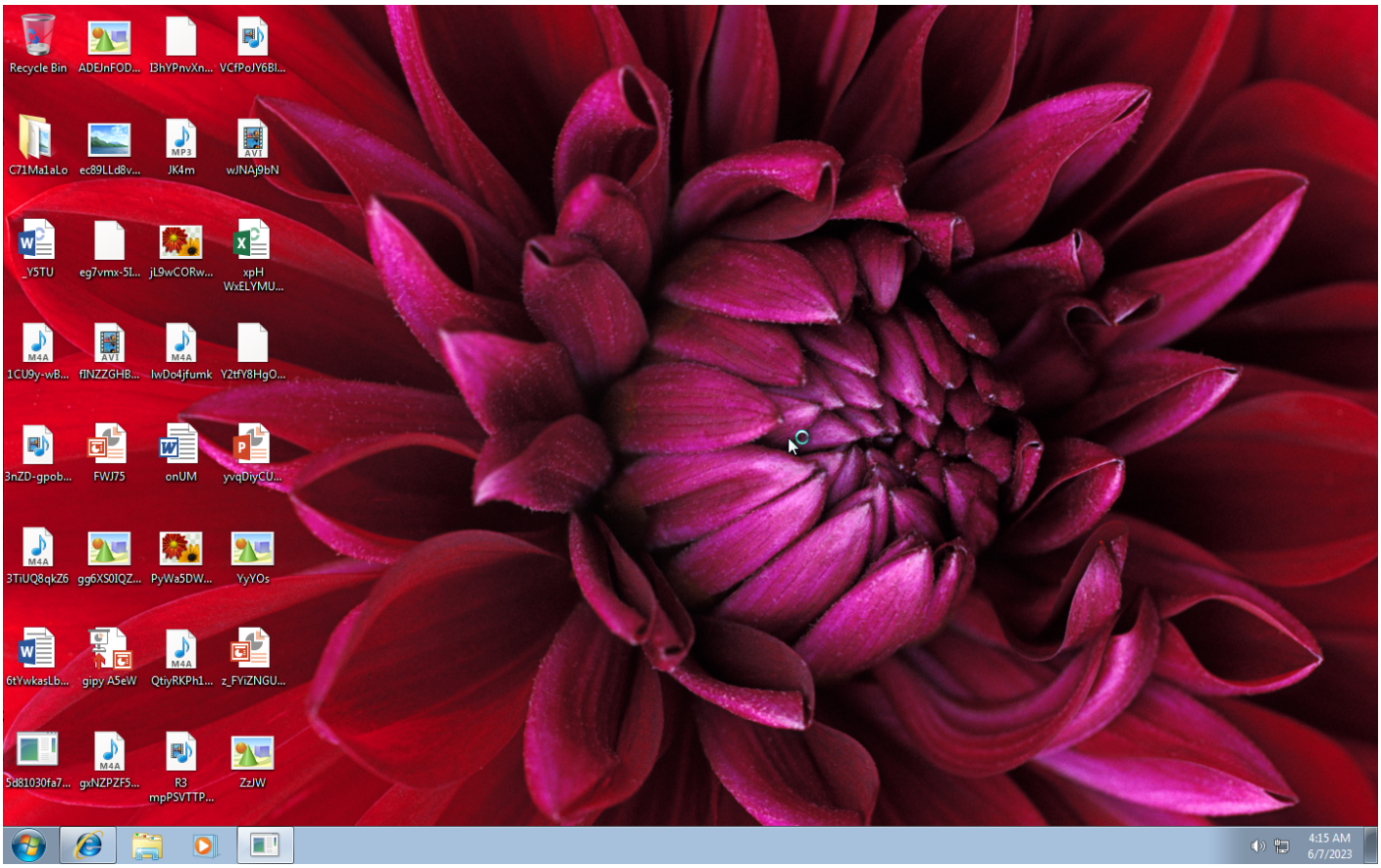
| | |
|---|---|
| ID | #7980375 |
| MD5 | 2bbff2111232d73a93cd435300d0a07e |
| SHA1 | b93d633d379052f0a15b0f9c7094829461a86dbb |
| SHA256 | 3160b4308dd9434ebb99e5747ec90d63722a640d329384b1ed536b59352dace6 |
| SSDeep | 49152:B+CUkw0e9xep5A4354qUoJo5DtjDgk9bcnfoEKSMBB90hMhlqTO4rpun4I:4CVG9y5ASUoJo5D5DgmbKfotB902QTOw |
| ImpHash | 6ed4f5f04d62b18d96b26d6db7c18840 |
| File Name | 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe |
| File Size | 2542.00 KB |
| Sample Type | Windows Exe (x86-64) |
| Has Macros | ✔ |

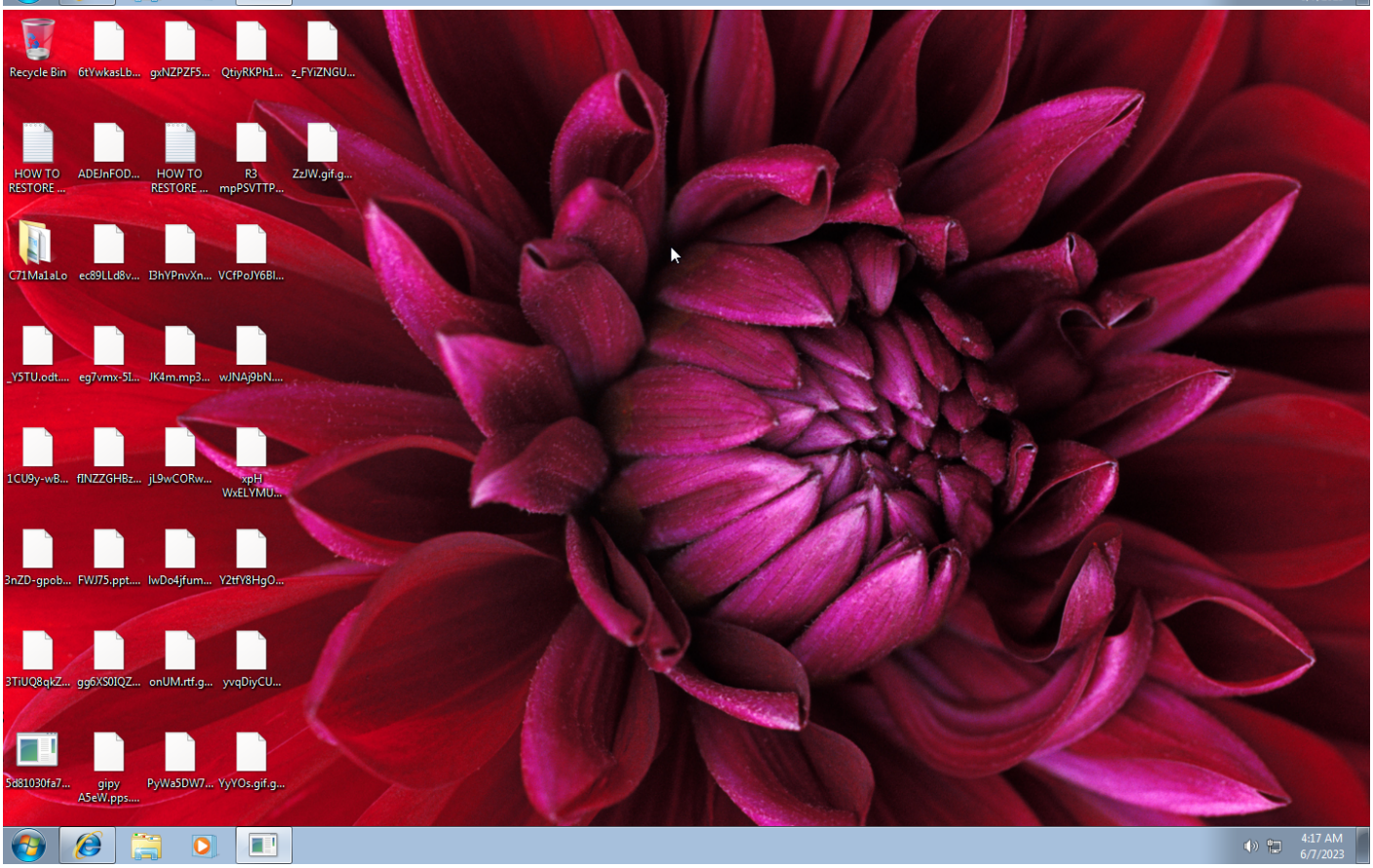
## Analysis Information

| | |
|---|---|
| Creation Time | 2023-06-07 02:15 (UTC) |
| Analysis Duration | 00:04:00 |
| Termination Reason | Timeout |
| Number of Monitored Processes | 9 |
| Execution Successful | False |
| Reputation Enabled | ✔ |
| WHOIS Enabled | ✔ |
| Built-in AV Enabled | ✖ |
| Built-in AV Applied On | Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files |
| Number of AV Matches | 0 |
| YARA Enabled | ✔ |
| YARA Applied On | Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files |
| Number of YARA Matches | 19 |


Recycle Bin
ADEInFOD...
I3hYPnvXn...
VCfPoJY6Bl...
C71Ma1aLo
ec89LLd8v...
JK4m
wJNAj9bN
_Y5TU
eg7vmx-5I...
jL9wCORw...
xpH WxELYMU...
1CU9y-wB...
fINZZGHB...
lwDo4jfumk
Y2tfY8HgO...
3nZD-gpob...
FWJ75
onUM
yvqDiyCU...
3TiUQ8qkZ6
gg6XS0IQZ...
PyWa5DW...
YyYOs
6tYwkasLb...
gipy A5eW
QtiyRKPh1...
z_FYiZNGU...
5d81030fa7...
gxNZPZF5...
R3 mpPSVTTP...
ZzJW
4:15 AM
6/7/2023


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: 5d81030fa79538850bef6375df9bdaebffd251271a04b9...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear




Screenshots truncated

# NETWORK

## General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

## DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

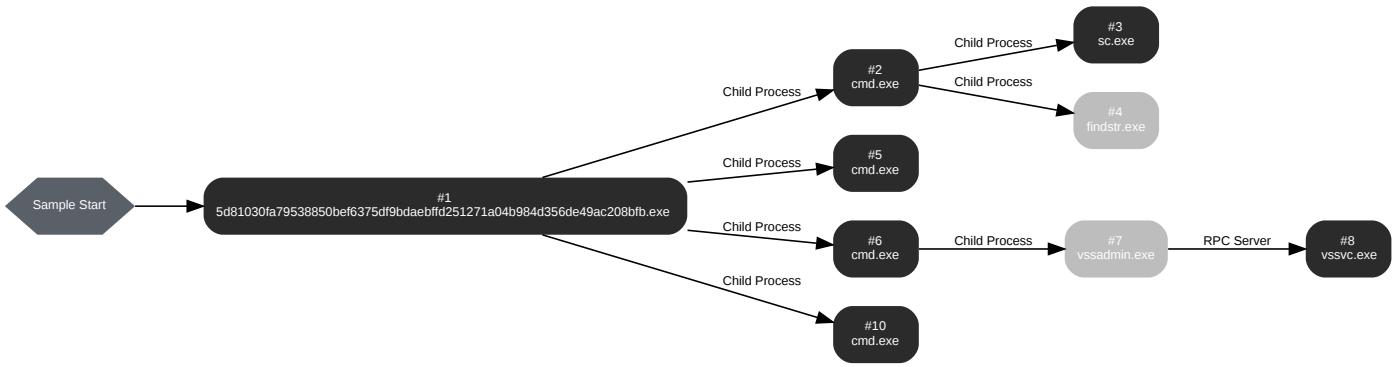
## HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

## BEHAVIOR

### Process Graph



### Process #1: 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe

| | |
|---|---|
| ID | 1 |
| File Name | c:\users\keecfmwgj\desktop\5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe |
| Command Line | "C:\Users\kEecfMwgj\Desktop\5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe" |
| Initial Working Directory | C:\Users\kEecfMwgj\Desktop\ |
| Monitor Start Time | Start Time: 36738, Reason: Analysis Target |
| Unmonitor End Time | End Time: 242910, Reason: Terminated |
| Monitor duration | 206.17s |
| Return Code | 0 |
| PID | 2688 |
| Parent PID | 1908 |
| Bitness | 64 Bit |

### Dropped Files (4)

| File Name | File Size | SHA256 | YARA Match |
|---|---|---|---|
| C:\Program Files\Java\jre1.8.0_171\lib\fonts\HOW TO RESTORE YOUR FILES.TXT | 758 bytes | 8104414020397799ae6c4f779a8486a8a5c2975f4a5cee250151ccfa9911f8ab | ✖ |
| C:\Users\kEecfMwgj\Desktop\scdamhjrnwsajyc.bat | 43 bytes | 1fbdb97893d09d59575c3ef95df3c929fe6b6ddf1b273283e4efadf94cdc802d | ✖ |
| c:\users\keecfmwgj\pictures\nxz1anlj8jy\ptvvv4hy6spvi\73u0fa3zn\mmlw_2ov6hiux\ciktxpdg4adjzbqf.gif.gdjlosvtnib | 0 bytes | e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 | ✖ |
| C:\Users\kEecfMwgj\Desktop\wbolds.bat | 47 bytes | 0965cb8ee38adedd9ba06bdad9220a35890c2df0e4c78d0559cd6da653bf740f | ✖ |

### Host Behavior

| Type | Count |
|---|---|
| Module | 104 |
| System | 5049 |
| Environment | 9 |
| - | 62 |
| File | 30724 |
| - | 111 |
| Process | 4 |

### Process #2: cmd.exe

| | |
|---|---|
| ID | 2 |
| File Name | c:\windows\system32\cmd.exe |
| Command Line | C:\Windows\system32\cmd.exe /c C:\Users\kEecfMwgj\Desktop\scdamhjrnwsajyc.bat |
| Initial Working Directory | C:\Users\kEecfMwgj\Desktop\ |
| Monitor Start Time | Start Time: 46578, Reason: Child Process |
| Unmonitor End Time | End Time: 48345, Reason: Terminated |
| Monitor duration | 1.77s |
| Return Code | 0 |
| PID | 2716 |
| Parent PID | 2688 |
| Bitness | 64 Bit |

### Host Behavior

| Type | Count |
|---|---|
| Module | 5 |
| Environment | 13 |
| File | 65 |
| Process | 2 |

### Process #3: sc.exe

| | |
|---|---|
| ID | 3 |
| File Name | c:\windows\system32\sc.exe |
| Command Line | SC QUERY |
| Initial Working Directory | C:\Users\kEecfMwgj\Desktop\ |
| Monitor Start Time | Start Time: 47085, Reason: Child Process |
| Unmonitor End Time | End Time: 47809, Reason: Terminated |
| Monitor duration | 0.72s |
| Return Code | 0 |
| PID | 2740 |
| Parent PID | 2716 |
| Bitness | 64 Bit |

### Host Behavior

| Type | Count |
|---|---|
| System | 3 |
| Module | 1 |
| File | 93 |
| - | 3 |

### Process #4: findstr.exe

| | |
|---|---|
| ID | 4 |
| File Name | c:\windows\system32\findstr.exe |
| Command Line | FINDSTR SERVICE_NAME |
| Initial Working Directory | C:\Users\kEecfMwgj\Desktop\ |
| Monitor Start Time | Start Time: 47157, Reason: Child Process |
| Unmonitor End Time | End Time: 48345, Reason: Terminated |
| Monitor duration | 1.19s |
| Return Code | 0 |
| PID | 2808 |
| Parent PID | 2716 |
| Bitness | 64 Bit |

### Process #5: cmd.exe

| | |
|---|---|
| ID | 5 |
| File Name | c:\windows\system32\cmd.exe |
| Command Line | C:\Windows\system32\cmd.exe /c C:\Users\kEecfMwgj\Desktop\wbolds.bat |
| Initial Working Directory | C:\Users\kEecfMwgj\Desktop\ |
| Monitor Start Time | Start Time: 47810, Reason: Child Process |
| Unmonitor End Time | End Time: 49283, Reason: Terminated |
| Monitor duration | 1.47s |
| Return Code | 1 |
| PID | 2820 |
| Parent PID | 2688 |
| Bitness | 64 Bit |

### Host Behavior

| Type | Count |
|---|---|
| Module | 1 |
| Environment | 1 |
| File | 10 |

### Process #6: cmd.exe

| | |
|---|---|
| ID | 6 |
| File Name | c:\windows\system32\cmd.exe |
| Command Line | C:\Windows\system32\cmd.exe /c C:\Users\kEecfMwgj\Desktop\mcdnrgijbptrsp.bat |
| Initial Working Directory | C:\Users\kEecfMwgj\Desktop\ |
| Monitor Start Time | Start Time: 197599, Reason: Child Process |
| Unmonitor End Time | End Time: 241589, Reason: Terminated |
| Monitor duration | 43.99s |
| Return Code | 0 |
| PID | 2720 |
| Parent PID | 2688 |
| Bitness | 64 Bit |

### Host Behavior

| Type | Count |
|---|---|
| Module | 5 |
| Environment | 11 |
| File | 50 |
| Process | 1 |

### Process #7: vssadmin.exe

| | |
|---|---|
| ID | 7 |
| File Name | c:\windows\system32\vssadmin.exe |
| Command Line | vssadmin delete shadows /all /quiet |
| Initial Working Directory | C:\Users\kEecfMwgj\Desktop\ |
| Monitor Start Time | Start Time: 198382, Reason: Child Process |
| Unmonitor End Time | End Time: 241545, Reason: Terminated |
| Monitor duration | 43.16s |
| Return Code | 0 |
| PID | 2824 |
| Parent PID | 2720 |
| Bitness | 64 Bit |

### Process #8: vssvc.exe

| | |
|---|---|
| ID | 8 |
| File Name | c:\windows\system32\vssvc.exe |
| Command Line | C:\Windows\system32\vssvc.exe |
| Initial Working Directory | C:\Windows\system32\ |
| Monitor Start Time | Start Time: 200053, Reason: RPC Server |
| Unmonitor End Time | End Time: 287377, Reason: Terminated by timeout |
| Monitor duration | 87.32s |
| Return Code | Unknown |
| PID | 2388 |
| Parent PID | 2824 |
| Bitness | 64 Bit |

### Host Behavior

| Type | Count |
|---|---|
| System | 3 |

### Process #10: cmd.exe

| | |
|---|---|
| ID | 10 |
| File Name | c:\windows\system32\cmd.exe |
| Command Line | C:\Windows\system32\cmd.exe /c C:\Users\kEecfMwgj\Desktop\xfbvIrrnkpmkoman.bat |
| Initial Working Directory | C:\Users\kEecfMwgj\Desktop\ |
| Monitor Start Time | Start Time: 241376, Reason: Child Process |
| Unmonitor End Time | End Time: 242910, Reason: Terminated |
| Monitor duration | 1.53s |
| Return Code | 1 |
| PID | 156 |
| Parent PID | 2688 |
| Bitness | 64 Bit |

### Host Behavior

| Type | Count |
|---|---|
| Module | 1 |
| Environment | 1 |
| File | 10 |

# ARTIFACTS

## File

| SHA256 | File Names | Category | File Size | MIME Type | Operations | Verdict |
|---|---|---|---|---|---|---|
| db67c1d987af9a6e574a1c1fc76118a2a267296e7a37e054309d101da4d46cd7 | - | Memory Dump | 4888.00 KB | application/vnd.microsoft.portable-executable | - | MALICIOUS |
| f9145dca3345c815fbe85c7df3f859e941e64dc477b585536c163488971418f7 | - | Memory Dump | 4888.00 KB | application/vnd.microsoft.portable-executable | - | MALICIOUS |
| 9b50b0b64aa2f5f05ed1e2fdf7c1e99fdf6f65fbd9b7a1e532bdf62266142083 | - | Memory Dump | 4888.00 KB | application/vnd.microsoft.portable-executable | - | MALICIOUS |
| df5f539cd3bbb5fc8c98bd569ef5cfbf3f862cfa0f74038c47f9f147ada2b58d | - | Memory Dump | 4888.00 KB | application/vnd.microsoft.portable-executable | - | MALICIOUS |
| 21fa3ad06b840976718eb1ec2491d2857fc6ef15d35276d14e7f2992d8da322b | - | Memory Dump | 4888.00 KB | application/vnd.microsoft.portable-executable | - | MALICIOUS |
| dba17b20941dbf1bf052b8788932e2f6a862bce9f3946f8872d63d1ac4773f4d | - | Memory Dump | 4888.00 KB | application/vnd.microsoft.portable-executable | - | MALICIOUS |
| 03f659f0476f3f78c023dbb644b1c4d6f40f6e5047e5e7750d5634fb99a7b2b4 | - | Memory Dump | 4888.00 KB | application/vnd.microsoft.portable-executable | - | MALICIOUS |
| 3160b4308dd9434ebb99e5747ec90d63722a640d329384b1ed536b59352dace6 | C:\Users\kEecfMwgj\Desktop\5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe | Sample File | 2542.00 KB | application/vnd.microsoft.portable-executable | Access | MALICIOUS |
| e814ac4aff1029e8a452ca7275c8a44205e0bf8cf80fc1b16d04e8e30a571610 | - | Memory Dump | 4888.00 KB | application/vnd.microsoft.portable-executable | - | MALICIOUS |
| 50c536f7f71ecfa660fcaff7efe9e0205ee3424ffac118df3d8750ffd9698059 | - | Memory Dump | 4888.00 KB | application/vnd.microsoft.portable-executable | - | MALICIOUS |
| 076923fc202f490f9d7eda6e443b5422dc690f0d5e5ce65d3001ab0ad43e74dd | - | Memory Dump | 4888.00 KB | application/vnd.microsoft.portable-executable | - | MALICIOUS |
| 1e76232d37d75d09f42d14756e6dfc9dbd26cdccbaa43d4c58677fbf9a9ccf0e | - | Memory Dump | 4888.00 KB | application/vnd.microsoft.portable-executable | - | MALICIOUS |
| 5d3e2e5c0d0cf67964ed343cd6d87b528b12039ca134853a32ec0e4b7304089d | - | Memory Dump | 4888.00 KB | application/vnd.microsoft.portable-executable | - | MALICIOUS |
| 2c89138715b16809c086dda1fec5561c49fe59cbe411f8b8cd71ae9806945dd7 | - | Memory Dump | 4888.00 KB | application/vnd.microsoft.portable-executable | - | MALICIOUS |
| 5bb0c37e558a3e725a54b73571586cc07d079b4f9a67f239762afaa21aea4e51 | - | Memory Dump | 4888.00 KB | application/vnd.microsoft.portable-executable | - | MALICIOUS |
| 65ad2575a77667ab4df1193014a7b913b99a7d1876e4c847ab92a55a1d10e495 | - | Memory Dump | 4888.00 KB | application/vnd.microsoft.portable-executable | - | MALICIOUS |
| ca20454204bf5fc2b800a8404066b63dc4eb93214ec2e5e7661b2004a50fca55 | - | Memory Dump | 4888.00 KB | application/vnd.microsoft.portable-executable | - | MALICIOUS |
| 4ba418356a2b2724d5a0092263f0648937b03bea1400913b9ff99c6cc95aa3e1 | - | Memory Dump | 4888.00 KB | application/vnd.microsoft.portable-executable | - | MALICIOUS |
| 4c8b71d53c3a895a90ddb343bde3552ae2d97ea6ddd5a506e007b301648714ee | - | Memory Dump | 4888.00 KB | application/vnd.microsoft.portable-executable | - | MALICIOUS |
| bcd518572ef5aa575f6df2102c76297b91a0cc9a8cef19e576aa3650f03a4cbf | - | Memory Dump | 4888.00 KB | application/vnd.microsoft.portable-executable | - | MALICIOUS |

| SHA256 | File Names | Category | File Size | MIME Type | Operations | Verdict |
|---|---|---|---|---|---|---|
| 8104414020397799ae6c4f779a8486a8a5c2975f4a5cee250151ccfa9911f8ab | C:\Program Files\Java\jre1.8.0_171\lib\fonts\HOW TO RESTORE YOUR FILES.TXT, C:\ProgramData\Package Cache\54050A5F8AE7F0C56E553F009... ...kages\HOW TO RESTORE YOUR FILES.TXT, c:\users\keecfmwgj\appdata\local\microsoft\feeds cache\6asvn7j7\how to restore your files.txt | Dropped File | 758 bytes | text/plain | Access, Create, Write | SUSPICIOUS |
| 1fbdb97893d09d59575c3ef95df3c929fe6b6ddf1b273283e4efadf94cdc802d | C:\Users\kEecfMwgj\Desktop\scdamhjrnwsajyc.bat | Dropped File | 43 bytes | text/x-msdos-batch | Access, Create, Delete, Read, Write | CLEAN |
| 0965cb8ee38adedd9ba06bdad9220a35890c2df0e4c78d0559cd6da653bf740f | C:\Users\kEecfMwgj\Desktop\wbolds.bat | Dropped File | 47 bytes | text/x-msdos-batch | Access, Create, Delete, Write | CLEAN |

### Filename

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| c:\program files (x86)\microsoft office\office16\logoimages\outlooklogosmall.contrast-white_scale-140.png.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\addins\power view excel add-in\ru\powerviewres.ru.xap.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\SendTo\Mail Recipient.MAPIMail.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0185776.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\j0200189.wmf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Office16\ADDINS\Power View Excel Add-in\pl\PowerViewRes.pl.xap.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\BL00267_.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Office16\1033\PUBSPAPR\PDIR35F.GIF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\1033\setlang_col.hxt.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\forms\1033\signl.ico.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Office16\Groove\ToolIcons\MAIL.ICO.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\so00610_.wmf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\pswavy.wmf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\logoimages\winwordlogosmall.scale-80.png.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\users\keecfmwgj\favorites\links\web slice gallery.url.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\na02361_.wmf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\users\keecfmwgj\documents\fcjyo2yce.xls.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Users\kEecfMwgj\ntuser.dat.LOG1.gdjlosvtnib | Accessed File | Access, Create, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Office16\PAGESIZE\PGLBL010.XML.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0107288.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\bl00234_.wmf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| C:\Program Files (x86)\Microsoft Office\Office16\LogoImages\OutlookLogoSmall.contrast-black_scale-100.png.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\pagesize\pgmn011.xml.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\j0107512.wmf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\users\keecfmwgj\appdata\locallow\microsoft\cryptneturlcache\metadata\77ec63bda74bd0d0e0426dc8f8008506.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\1033\quickstyles\linesstylish.dotx.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0153518.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\users\public\pictures\sample pictures\lighthouse.jpg.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\j0152622.wmf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\document themes 16\theme colors\blue ii.xml.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\users\keecfmwgj\music\p-aht5euvmn9yg a\xogyrc9xeogfnxo0t\jqp0k4pbeegfyfj\5ojbjtm.mp3.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\FD02071_.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\groove\tooldata\groove.net\computers\computericonmask.bmp.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\users\public\pictures\sample pictures\jellyfish.jpg.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\pagesize\pglbl081.xml.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Office16\1033\PUBSPAPR\ZPDIR25F.GIF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\ED00019_.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0301432.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\1033\pubspapr\pdir39f.gif.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0152432.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\an04196_.wmf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0099173.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\j0152602.wmf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Stationery\1033\NOTEBOOK.HTM.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\users\public\pictures\sample pictures\chrysanthemum.jpg.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\pubwiz\flyerhm.poc.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\programdata\package cache\{65e650ff-30be-469d-b63a-418d71ea1765}\state.rsm.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\logoimages\excellogosmall.scale-140.png.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Office16\MEDIA\SUCTION.WAV.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| c:\program files (x86)\microsoft office\office16\addins\power view excel add-in\id\powerviewres.id.xap.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\1033\skypefb.hxs.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\logoimages\powerpntlogosmall.contrast-white_scale-140.png.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\templates\1033\access\part\tasks.accdt.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\so02263_.wmf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\TN01164_.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0157831.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\media\lync_ringtone7.wav.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Users\kEecfMwgj\AppData\Local\Microsoft\Office\OTele\{8136E16F-A709-48AC-A08D-98CF5E5DDCD4} (1) - 1908 - excel.exe - OTeleMediumCost.dat.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\an00965_.wmf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\wordcnvpxy.cnv.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\msipc\da\msipc.dll.mui.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0281243.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\logoimages\outlooklogo.scale-140.png.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\groove\tooldata\groove.net\commondata\alertimage_off.jpg.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\east_01.mid.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\j0400004.png.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\NA02444_.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\SO00671_.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Users\kEecfMwgj\AppData\Local\Microsoft\Media Player\LocalMLS_3.wmdb.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\programdata\microsoft help\ms.outlook.16.1033.hxn.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Office16\OutlookAutoDiscover\WANS.NET.XML.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Stationery\1033\DADSHIRT.GIF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Office16\LogoImages\VisioLogoSmall.contrast-black_scale-140.png.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Office16\1033\PUBFTSCM\SCHEME26.CSS.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\pubwiz\invite11.poc.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Users\kEecfMwgj\Desktop\C71Ma1aLo\fpe7qy-m.mp3.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\msipc\zh-tw\msipc.dll.mui.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| c:\program files (x86)\microsoft office\clipart\pub60cor\j0105250.wmf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\lync2013_third_party_notices.txt.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\outlookautodiscover\yahoo.co.jp.xml.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\SO00735_.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\na01152_.wmf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\forms\1033\taskupd.cfg.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\1033\pubftscm\scheme34.css.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files\java\jre1.8.0_171\lib\fonts\lucidatypewriterbold.ttf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0105710.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Users\kEecfMwgj\AppData\Local\Microsoft\Windows Mail\Stationery\HandPrints.jpg.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Templates\1033\TimelessResume.dotx.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\msocache\all users\{90160000-00e2-0409-0000-0000000ff1ce}-c\osmuxmui.msi.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\j0290548.wmf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\so00917_.wmf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Office16\CONVERT\OLJRNL.FAE.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Office16\PUBWIZ\DGWEBSBR.XML.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\AG00158_.GIF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\1033\pubspapr\zpdir50b.gif.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\ph02567j.jpg.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files\java\jre1.8.0_171\lib\jfxswt.jar.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Office16\LogoImages\WinWordLogoSmall.scale-180.png.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\j0105638.wmf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0145373.JPG.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Office16\PUBWIZ\SIGN98.POC.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\outlookautodiscover\yahoo.com.ar.xml.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0099180.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Office16\LogoImages\GrooveLogo.contrast-black_scale-180.png.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\j0341742.jpg.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| c:\program files (x86)\microsoft office\office16\1033\pubftscm\scheme46.css.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\msocache\all users\{90160000-00e1-0409-0000-0000000ff1ce}-c\osmmui.cab.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\WHIRL1.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\users\keecfmwgj\appdata\local\microsoft\office\otele\{3caf51ca-d3f9-4432-81a9-f56ac51caa37} (0) - 1920 - excel.exe - otelemediumcost.dat.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Office16\ADDINS\PowerPivot Excel Add-in\Cartridges\sql70.xsl.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Office16\OMML2MML.XSL.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\pubwiz\dgcoupon.dpv.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Office16\LogoImages\ExcelLogo.scale-140.png.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\BS00184_.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\users\keecfmwgj\appdata\locallow\microsoft\cryptneturlcache\metadata\c0018bb1b5834735bfa60cd063b31956.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Office16\PAGESIZE\PGMN002.XML.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\users\keecfmwgj\appdata\local\microsoft\outlook\roamcache\stream_availabilityoptions_2_75c5cb426a060443a982525df40ca7ef.dat.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\users\public\pictures\sample pictures\desert.jpg.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\logoimages\onenotelogo.scale-140.png.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\dd00117_.wmf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0187847.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\j0287415.wmf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\library\analysis\analys32.xll.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\j0282932.wmf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Libraries\Pictures.library-ms.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Office16\DCF\AccessMessageDismissal.txt.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\logoimages\visiologo.contrast-white_scale-140.png.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\FD02158_.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\logoimages\winprojlogo.contrast-white_scale-180.png.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0107134.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Users\kEecfMwgj\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00008B4D\02_Music_added_in_the_last_month.wpl.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| c:\program files (x86)\microsoft office\office16\addins\powerpivot excel add-in\resources\1060\powerpivotexcelclientaddin.rll.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\users\keecfmwgj\appdata\local\microsoft\onedrive\17.3.4604.0120\hi\filesync.localizedresources.dll.mui.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\NA00058_.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\j0186362.wmf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\users\keecfmwgj\desktop\c71ma1alo\05rfrauxo.flv.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\addins\power view excel add-in\eu\powerviewres.eu.xap.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\programdata\package cache\{2bc3bd4d-faba-4394-93c7-9ac82a263fe2}v14.25.28508\packages\vcruntimeminimum_x86\cab1.cab.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\addins\powerpivot excel add-in\zh-chs\localizedstrings.xml.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\DD01166_.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\na01472_.wmf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\media\lync_ringtone2.wav.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\dd01772_.wmf.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0197979.WMF.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\1033\pubftscm\scheme52.css.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\addins\powerpivot excel add-in\ar\localizedstrings.xml.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\users\keecfmwgj\appdata\locallow\microsoft\cryptneturlcache\content\57c8edb95df3f0ad4ee2dc2b8cfd4157.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\office16\addins\power view excel add-in\zh-chs\powerviewres.zh-chs.xap.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| C:\Program Files (x86)\Microsoft Office\Office16\OutlookAutoDiscover\PRODIGY.NET.XML.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |
| c:\program files (x86)\microsoft office\clipart\pub60cor\j0313974.jpg.gdjlosvtnib | Accessed File, Dropped File, Modified File | Access, Create, Read, Write | MALICIOUS |

## Reduced dataset

### Process

| Process Name | Commandline | Verdict |
|---|---|---|
| 5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe | "C:\Users\kEecfMwgj\Desktop\5d81030fa79538850bef6375df9bdaebffd251271a04b984d356de49ac208bfb.exe" | MALICIOUS |
| sc.exe | SC QUERY | SUSPICIOUS |
| cmd.exe | C:\Windows\system32\cmd.exe /c C:\Users\kEecfMwgj\Desktop\mcdnrgijbptrsp.bat | SUSPICIOUS |
| cmd.exe | C:\Windows\system32\cmd.exe /c C:\Users\kEecfMwgj\Desktop\scdamhjrnwsajyc.bat | CLEAN |
| findstr.exe | FINDSTR SERVICE_NAME | CLEAN |
| cmd.exe | C:\Windows\system32\cmd.exe /c C:\Users\kEecfMwgj\Desktop\wbolds.bat | CLEAN |
| vssadmin.exe | vssadmin delete shadows /all /quiet | CLEAN |
| vssvc.exe | C:\Windows\system32\vssvc.exe | CLEAN |

| Process Name | Commandline | Verdict |
|---|---|---|
| cmd.exe | C:\Windows\system32\cmd.exe /c C:\Users\kEecfMwgj\Desktop\xfbvlrrnkpmkoman.bat | CLEAN |

## YARA / AV

### YARA (19)

| Ruleset Name | Rule Name | Rule Description | File Type | File Name | Classification | Verdict |
|---|---|---|---|---|---|---|
| Ransomware | GoRansom | GoRansom Ransomware | Memory Dump | - | Ransomware | 5/5 |
| Ransomware | GoRansom | GoRansom Ransomware | Memory Dump | - | Ransomware | 5/5 |
| Ransomware | GoRansom | GoRansom Ransomware | Memory Dump | - | Ransomware | 5/5 |
| Ransomware | GoRansom | GoRansom Ransomware | Memory Dump | - | Ransomware | 5/5 |
| Ransomware | GoRansom | GoRansom Ransomware | Memory Dump | - | Ransomware | 5/5 |
| Ransomware | GoRansom | GoRansom Ransomware | Memory Dump | - | Ransomware | 5/5 |
| Ransomware | GoRansom | GoRansom Ransomware | Memory Dump | - | Ransomware | 5/5 |
| Ransomware | GoRansom | GoRansom Ransomware | Memory Dump | - | Ransomware | 5/5 |
| Ransomware | GoRansom | GoRansom Ransomware | Memory Dump | - | Ransomware | 5/5 |
| Ransomware | GoRansom | GoRansom Ransomware | Memory Dump | - | Ransomware | 5/5 |
| Ransomware | GoRansom | GoRansom Ransomware | Memory Dump | - | Ransomware | 5/5 |
| Ransomware | GoRansom | GoRansom Ransomware | Memory Dump | - | Ransomware | 5/5 |
| Ransomware | GoRansom | GoRansom Ransomware | Memory Dump | - | Ransomware | 5/5 |
| Ransomware | GoRansom | GoRansom Ransomware | Memory Dump | - | Ransomware | 5/5 |
| Ransomware | GoRansom | GoRansom Ransomware | Memory Dump | - | Ransomware | 5/5 |
| Ransomware | GoRansom | GoRansom Ransomware | Memory Dump | - | Ransomware | 5/5 |
| Ransomware | GoRansom | GoRansom Ransomware | Memory Dump | - | Ransomware | 5/5 |
| Ransomware | GoRansom | GoRansom Ransomware | Memory Dump | - | Ransomware | 5/5 |
| Ransomware | GoRansom | GoRansom Ransomware | Memory Dump | - | Ransomware | 5/5 |

# ENVIRONMENT

### Virtual Machine Information

| | |
|---|---|
| Name | win7_64_sp1_en_mso2016 |
| Description | win7_64_sp1_en_mso2016 |
| Architecture | x86 64-bit |
| Operating System | Windows 7 |
| Kernel Version | 6.1.7601.18741 (2e37f962-d699-492c-aaf3-f9f4e9770b1d) |
| Network Scheme Name | Local Gateway |
| Network Config Name | Local Gateway |

### Platform Information

| | |
|---|---|
| Platform Version | 2023.2.0 |
| Dynamic Engine Version | 2023.2.0 / 04/13/2023 04:20 |
| Static Engine Version | 2023.2.0.0 / 2023-04-13 03:00:20 |
| AV Exceptions Version | 2023.2.1.4 / 2023-04-17 18:38:13 |
| Link Detonation Heuristics Version | 2023.2.1.11 / 2023-05-25 14:08:46 |
| Smart Memory Dumping Rules Version | 2023.2.1.4 / 2023-04-17 18:38:13 |
| Config Extractors Version | 2023.2.1.11 / 2023-05-25 14:08:46 |
| Signature Trust Store Version | 2023.2.1.4 / 2023-04-17 18:38:13 |
| VMRay Threat Identifiers Version | 2023.2.1.13 / 2023-06-02 06:54:11 |
| YARA Built-in Ruleset Version | 2023.2.1.13 |

### Software Information

| | |
|---|---|
| Adobe Acrobat Reader Version | Not installed |
| Microsoft Office | 2016 |
| Microsoft Office Version | 16.0.4266.1001 |
| Hangul Office | Not installed |
| Hangul Office Version | Not installed |
| Internet Explorer Version | 8.0.7601.17514 |
| Chrome Version | Not installed |
| Firefox Version | Not installed |
| Flash Version | Not installed |
| Java Version | 8.0.1710.11 |

### System Information

| | |
|---|---|
| Sample Directory | C:\Users\kEecfMwgj\Desktop |
| Computer Name | Q9IATRKPRH |
| User Domain | Q9IATRKPRH |
| User Name | kEecfMwgj |
| User Profile | C:\Users\kEecfMwgj |
| Temp Directory | C:\Users\KEECFM~1\AppData\Local\Temp |

| | |
|---|---|
| System Root | C:\Windows |