**MALICIOUS**

Classifications: -

Threat Names: Mal/Generic-S RedNet

Verdict Reason: -

| | |
|---|---|
| **Sample Type** | **Windows Exe (x86-32)** |
| **File Name** | **be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe** |
| ID | #4211439 |
| MD5 | 17f97f9c91b0daf856526130cf9bd702 |
| SHA1 | 268685c49e0bc50f7a7e977d2d71768a1e958f03 |
| SHA256 | be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8 |
| File Size | 221.00 KB |
| Report Created | 2022-04-28 15:47 (UTC+2) |
| Target Environment | win10_64_th2_en_mso2016 \| exe |

# OVERVIEW

## VMRay Threat Identifiers (9 rules, 110 matches)

| Score | Category | Operation | Count | Classification |
|---|---|---|---|---|
| 5/5 | User Data Modification | Renames user files | 1 | Ransomware |
| | • (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe renames multiple user files. | | | |
| 5/5 | YARA | Malicious content matched by YARA rules | 2 | - |
| | • Rule "Packer_RedNet" from ruleset "Generic" has matched on a memory dump for (process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe.<br>• Rule "Packer_RedNet" from ruleset "Generic" has matched on the sample itself. | | | |
| 5/5 | User Data Modification | Modifies Windows automatic backups | 1 | - |
| | • (Process #2) cmd.exe deletes Windows volume shadow copies. | | | |
| 4/5 | Reputation | Known malicious file | 2 | - |
| | • File "C:\Users\Public\sys.bat" is a known malicious file.<br>• Reputation analysis labels the sample itself as Mal/Generic-S. | | | |
| 2/5 | Data Collection | Reads sensitive ftp data | 1 | - |
| | • (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe tries to read sensitive data of ftp application "AbleFTP" by file. | | | |
| 2/5 | Hide Tracks | Deletes file after execution | 1 | - |
| | • (Process #4) cmd.exe deletes executed executable "c:\users\rdhj0cnfevzx\desktop\be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe". | | | |
| 1/5 | Privilege Escalation | Enables process privilege | 1 | - |
| | • (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe enables process privilege "SeDebugPrivilege". | | | |
| 1/5 | Hide Tracks | Creates process with hidden window | 1 | - |
| | • (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe starts (process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe with a hidden window. | | | |
| 1/5 | System Modification | Modifies application directory | 100 | - |

- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\n_nxg3 tg8vt.jpg[newpatek@cock.li].marra".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\clicktorun\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\clicktorun\c2rheartbeatconfig.xml[newpatek@cock.li].marra".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\clicktorun\officeupdateschedule.xml[newpatek@cock.li].marra".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\clicktorun\servicewatcherschedule.xml[newpatek@cock.li].marra".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\ar-sa\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\bg-bg\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\cs-cz\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\da-dk\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\de-de\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\el-gr\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\en-gb\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\es-es\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\es-mx\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\et-ee\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\fi-fi\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\fr-ca\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\auxpad\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\insert\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\keypad\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\main\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\oskclearui\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\oskmenu\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\osknav\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\osknumpad\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\oskpred\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\symbols\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\he-il\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\hr-hr\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\hu-hu\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\hwrcustomization\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\it-it\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\ja-jp\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\ko-kr\marracrypt_information.html".
- (Process #1) be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe modifies "c:\program files\common files\microsoft shared\ink\languagemodel\marracrypt_information.html".

### Mitre ATT&CK Matrix

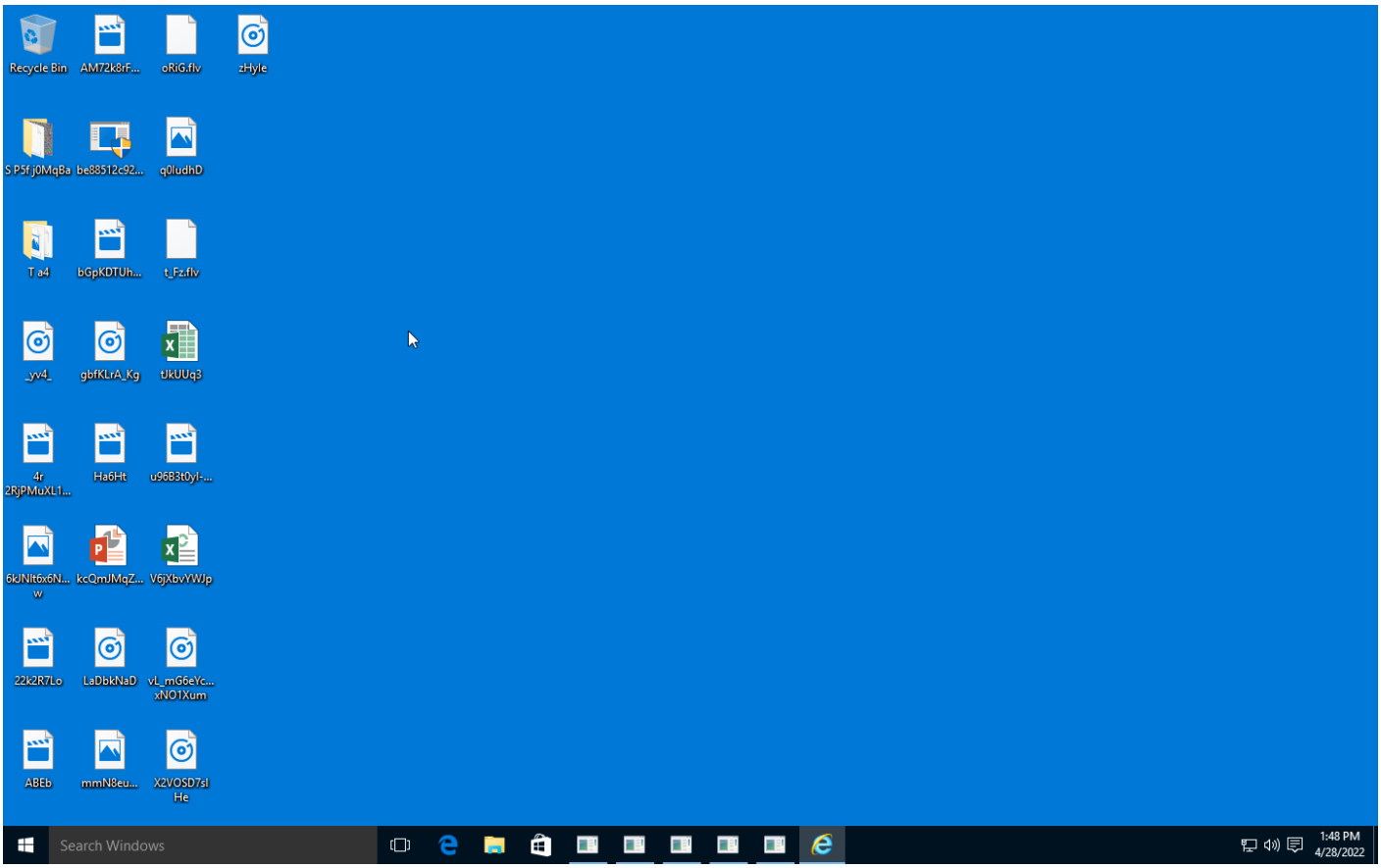
| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | #T1143 Hidden Window | #T1081 Credentials in Files | #T1083 File and Directory Discovery | | #T1119 Automated Collection | | | #T1486 Data Encrypted for Impact |
| | | | | | | | | #T1005 Data from Local System | | | #T1490 Inhibit System Recovery |

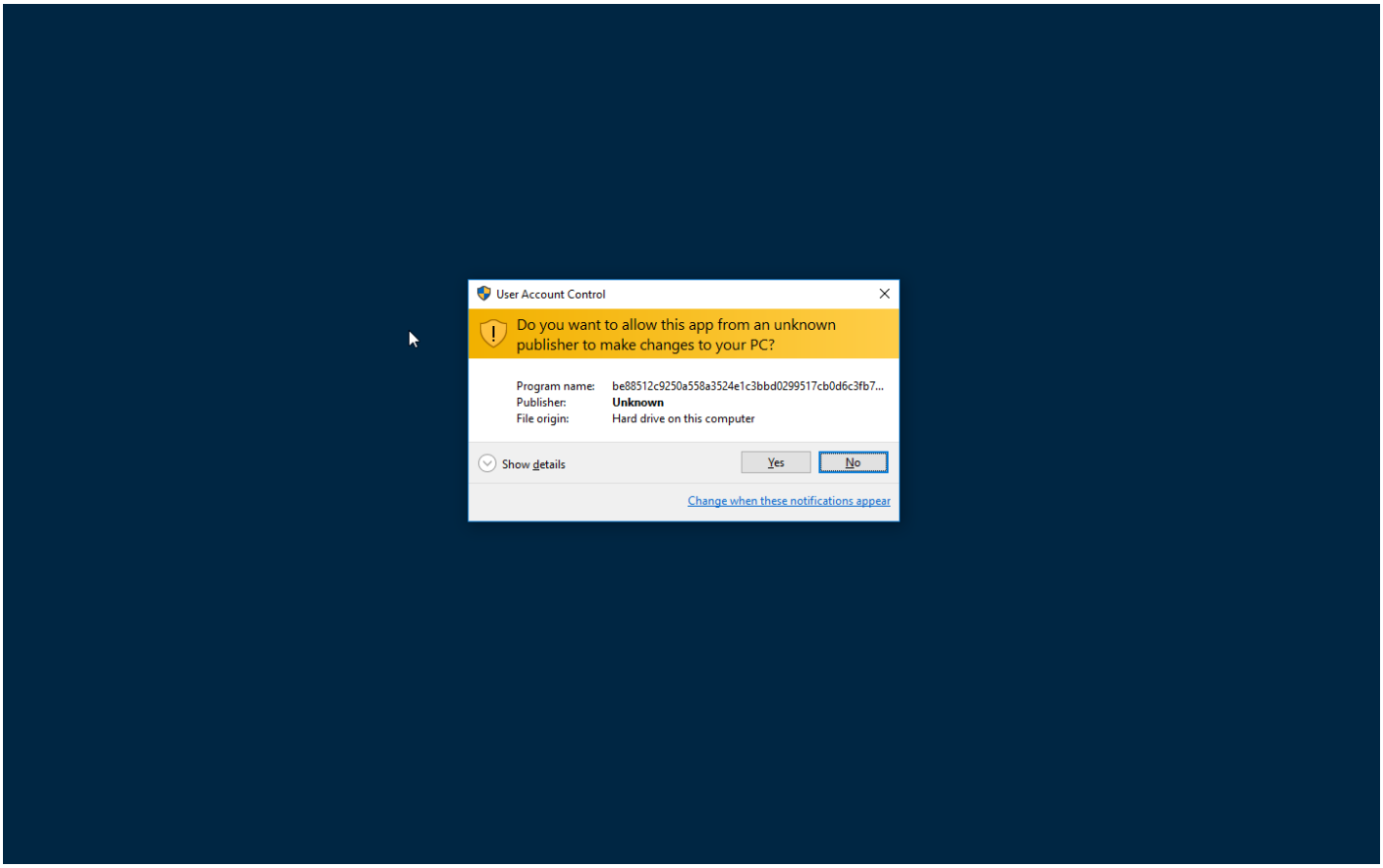
## Sample Information

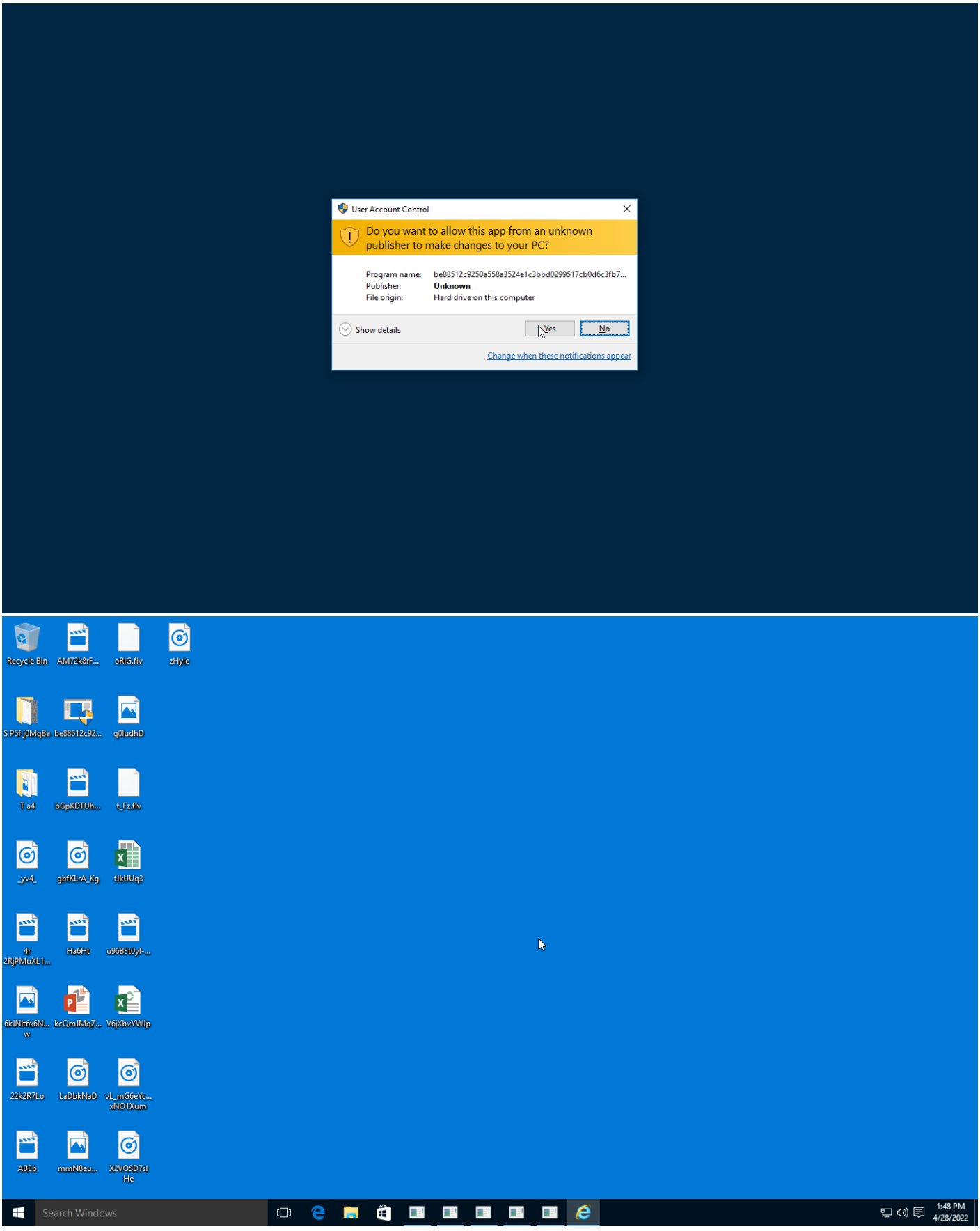
| | |
|---|---|
| ID | #4211439 |
| MD5 | 17f97f9c91b0daf856526130cf9bd702 |
| SHA1 | 268685c49e0bc50f7a7e977d2d71768a1e958f03 |
| SHA256 | be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8 |
| SSDeep | 6144:adSK04ETTZ+4TBpvjLCQHlJUgvoAbcz+w:aoL4EnU4T/vjLhnlv1bBw |
| ImpHash | 9dd8c0ff4fc84287e5b766563240f983 |
| File Name | be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe |
| File Size | 221.00 KB |
| Sample Type | Windows Exe (x86-32) |
| Has Macros | ✔ |

## Analysis Information

| | |
|---|---|
| Creation Time | 2022-04-28 15:47 (UTC+2) |
| Analysis Duration | 00:03:47 |
| Termination Reason | Maximum binlog size reached |
| Number of Monitored Processes | 19 |
| 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 | 3 |


Recycle Bin
AM72k8rF...
oRiG.flv
zHyIe
S P5f j0MqBa
be88512c92...
q0IudhD
T a4
bGpKDTUh...
t_Fz.flv
_yv4_
gbfKLrA_Kg
tJkUUq3
4r 2RjPMuXL1...
Ha6Ht
u96B3t0yI-...
6kjNIt6x6N... w
kcQmJMqZ...
V6jXbvYWJp
22k2R7Lo
LaDbkNaD
vL_mG6eYc... xNO1Xum
ABEb
mmN8eu...
X2VOSD7sI He
Search Windows
1:48 PM
4/28/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb7...
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

1 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

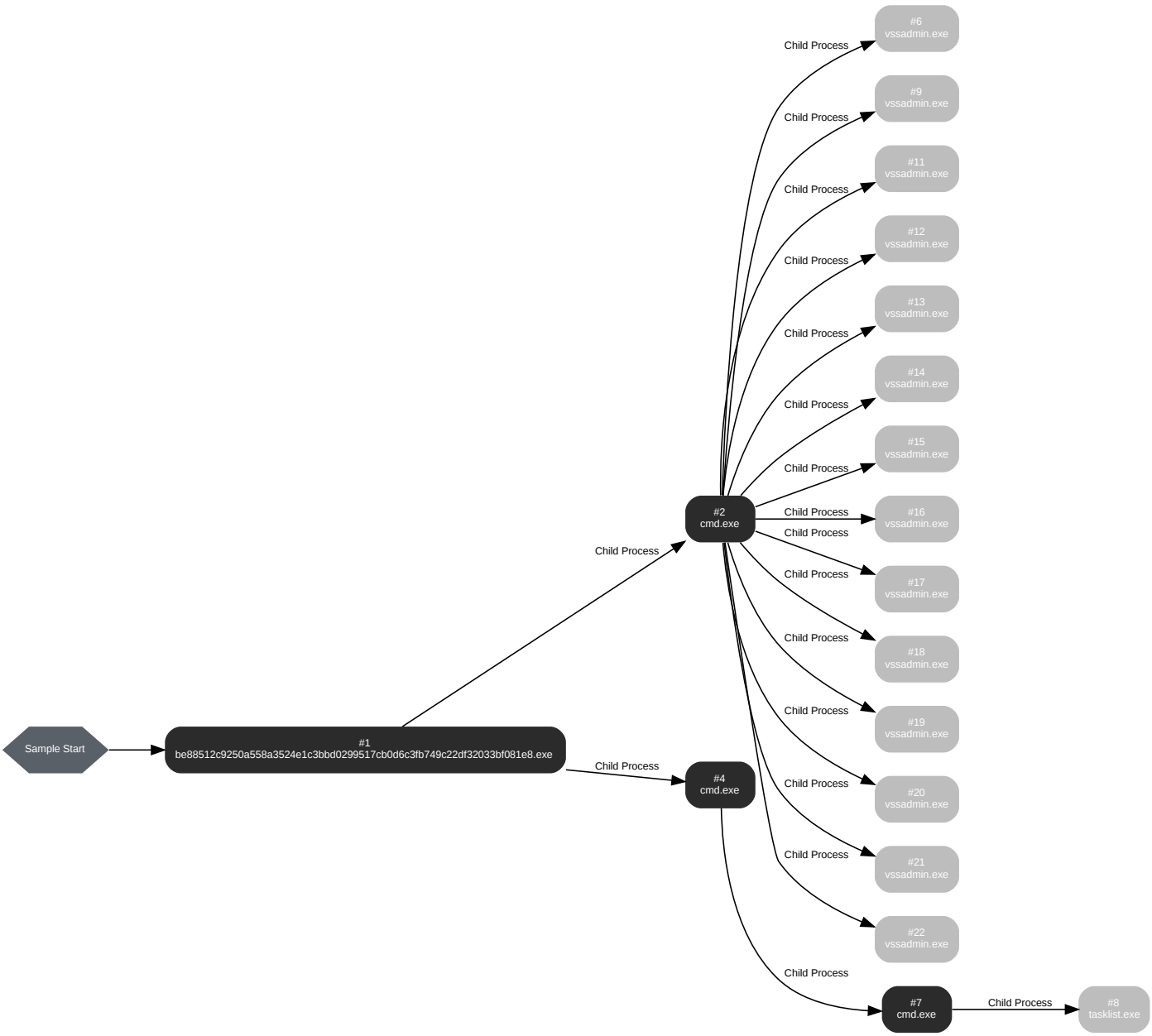
0 sessions, 0 bytes sent, 0 bytes received

## HTTP Requests

| Method | URL | Dest. IP | Dest. Port | Status Code | Response Size | Verdict |
|---|---|---|---|---|---|---|
| GET | https://www.bestbitcoinexchange.io | - | - | | 0 bytes | NA |

## BEHAVIOR

### Process Graph



### Process #1: be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe

| | |
|---|---|
| ID | 1 |
| File Name | c:\users\rdhj0cnfevzx\desktop\be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe |
| Command Line | "C:\Users\RDhJ0CNFevzX\Desktop\be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe" |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 74250, Reason: Analysis Target |
| Unmonitor End Time | End Time: 301847, Reason: Terminated by timeout |
| Monitor duration | 227.60s |
| Return Code | Unknown |
| PID | 2308 |
| Parent PID | 1932 |
| Bitness | 32 Bit |

### Dropped Files (10)

| File Name | File Size | SHA256 | YARA Match |
|---|---|---|---|
| C:\Program Files\Common Files\microsoft shared\ClickToRun\ServiceWatcherSchedule.xml[newpatek@cock.li].MARRA | 4.61 KB | fa7943a3aed783cd7ed4c6e95be582876c1f02c21204721d216eff2597962cdb | ✖ |
| C:\Users\Public\MARRACRYPT_ID_DO_NOT_TOUCH | 1.66 KB | 75ceb6d60b0abf24795bd77de0fc9b8f9958638bf111f04e831714a34b3bebb47 | ✖ |
| C:\Users\Public\PUBLIC_KEY_DO_NOT_TOUCH | 276 bytes | cc1d60af1cc96282afa832d3f65cacbcc612c47e00d2006beb5949b144d1638e | ✖ |
| C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeUpdateSchedule.xml[newpatek@cock.li].MARRA | 4.94 KB | 6e110d252e956412713fcc9b7fa0cb6b195a6d662651635629e44a7d101e0b52 | ✖ |
| C:\Program Files\Common Files\n_NxG3TG8VT.jpg[newpatek@cock.li].MARRA | 25.58 KB | ab87b945b4cd562202394bf73e6fd2f604a6ffdb3b31307418ba47d9b8cfd7b3 | ✖ |
| C:\Program Files\Common Files\microsoft shared\ClickToRun\C2RHeartbeatConfig.xml[newpatek@cock.li].MARRA | 4.31 KB | 037632396b47ec22658e15758a6a1b7357b1a39703f8eafe9e0cf6bc0bc0024d | ✖ |
| C:\Users\Public\MARRACRYPT_ID_DO_NOT_TOUCH | 1.14 KB | b8c94f3f2f59902accf583a1d63607d4edd6b74f32ff46d6562fd9774e472997 | ✖ |
| C:\Boot\MARRACRYPT_INFORMATION.HTML | 6.24 KB | 88f0015ad381b66e803842931dda2704b5d0076392f69b66e8a964e222e3cc8d | ✖ |
| C:\Program Files\Common Files\System\msadc\MARRACRYPT_INFORMATION.HTML | 0 bytes | e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 | ✖ |
| C:\Program Files\Windows Media Player\en-US\MARRACRYPT_INFORMATION.HTML | 0 bytes | e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 | ✖ |

### Host Behavior

| Type | Count |
|---|---|
| File | 21118 |
| Module | 88 |
| Environment | 1 |
| System | 6 |
| Process | 2 |
| User | 1 |

### Process #2: cmd.exe

| | |
|---|---|
| ID | 2 |
| File Name | c:\windows\syswow64\cmd.exe |
| Command Line | "cmd.exe" /C "C:\Users\Public\sys.bat" |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 118937, Reason: Child Process |
| Unmonitor End Time | End Time: 301847, Reason: Terminated by timeout |
| Monitor duration | 182.91s |
| Return Code | Unknown |
| PID | 3640 |
| Parent PID | 2308 |
| Bitness | 32 Bit |

### Dropped Files (1)

| File Name | File Size | SHA256 | YARA Match |
|---|---|---|---|
| C:\Users\Public\sys.bat | 1.48 KB | 8940135a58d28338ce4ea9b9933e6780507c56ab37a2f2e3a1a98c6564548a12 | ✖ |

### Host Behavior

| Type | Count |
|---|---|
| Environment | 167 |
| File | 6990 |
| Registry | 17 |
| Module | 8 |
| Process | 14 |
| System | 1 |

### Process #4: cmd.exe

| | |
|---|---|
| ID | 4 |
| File Name | c:\windows\syswow64\cmd.exe |
| Command Line | C:\Windows\system32\cmd.exe /c ""C:\ProgramData\newpatek\onmywrist.bat"" |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 119780, Reason: Child Process |
| Unmonitor End Time | End Time: 156912, Reason: Terminated |
| Monitor duration | 37.13s |
| Return Code | 1 |
| PID | 1832 |
| Parent PID | 2308 |
| Bitness | 32 Bit |

### Dropped Files (1)

| File Name | File Size | SHA256 | YARA Match |
|---|---|---|---|
| C:\ProgramData\newpatek\onmywrist.bat | 346 bytes | 75f25a3c2d1383ff052b7848e1133c383075e8f65b8a70eb2fd49321dcf076b0 | ✖ |

### Host Behavior

| Type | Count |
|---|---|
| Process | 1 |
| File | 165 |
| Environment | 25 |
| Registry | 17 |
| System | 1 |
| Module | 8 |

### Process #6: vssadmin.exe

| | |
|---|---|
| ID | 6 |
| File Name | c:\windows\syswow64\vssadmin.exe |
| Command Line | vssadmin Delete Shadows /all /quiet |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 136629, Reason: Child Process |
| Unmonitor End Time | End Time: 144918, Reason: Terminated |
| Monitor duration | 8.29s |
| Return Code | 2 |
| PID | 864 |
| Parent PID | 3640 |
| Bitness | 32 Bit |

### Process #7: cmd.exe

| | |
|---|---|
| ID | 7 |
| File Name | c:\windows\syswow64\cmd.exe |
| Command Line | C:\Windows\system32\cmd.exe /c tasklist /NH /FI "IMAGENAME eq be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe" |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 138826, Reason: Child Process |
| Unmonitor End Time | End Time: 154033, Reason: Terminated |
| Monitor duration | 15.21s |
| Return Code | 0 |
| PID | 3768 |
| Parent PID | 1832 |
| Bitness | 32 Bit |

### Host Behavior

| Type | Count |
|---|---|
| Module | 8 |
| Registry | 17 |
| Environment | 17 |
| File | 11 |
| Process | 1 |
| System | 1 |

### Process #8: tasklist.exe

| | |
|---|---|
| ID | 8 |
| File Name | c:\windows\syswow64\tasklist.exe |
| Command Line | tasklist /NH /FI "IMAGENAME eq be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe" |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 140353, Reason: Child Process |
| Unmonitor End Time | End Time: 155006, Reason: Terminated |
| Monitor duration | 14.65s |
| Return Code | 0 |
| PID | 316 |
| Parent PID | 3768 |
| Bitness | 32 Bit |

### Process #9: vssadmin.exe

| | |
|---|---|
| ID | 9 |
| File Name | c:\windows\syswow64\vssadmin.exe |
| Command Line | vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 146697, Reason: Child Process |
| Unmonitor End Time | End Time: 153449, Reason: Terminated |
| Monitor duration | 6.75s |
| Return Code | 2 |
| PID | 564 |
| Parent PID | 3640 |
| Bitness | 32 Bit |

### Process #11: vssadmin.exe

| | |
|---|---|
| ID | 11 |
| File Name | c:\windows\syswow64\vssadmin.exe |
| Command Line | vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 154530, Reason: Child Process |
| Unmonitor End Time | End Time: 156774, Reason: Terminated |
| Monitor duration | 2.24s |
| Return Code | 2 |
| PID | 3940 |
| Parent PID | 3640 |
| Bitness | 32 Bit |

### Process #12: vssadmin.exe

| | |
|---|---|
| ID | 12 |
| File Name | c:\windows\syswow64\vssadmin.exe |
| Command Line | vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 156745, Reason: Child Process |
| Unmonitor End Time | End Time: 159333, Reason: Terminated |
| Monitor duration | 2.59s |
| Return Code | 2 |
| PID | 5100 |
| Parent PID | 3640 |
| Bitness | 32 Bit |

### Process #13: vssadmin.exe

| | |
|---|---|
| ID | 13 |
| File Name | c:\windows\syswow64\vssadmin.exe |
| Command Line | vssadmin resize shadowstorage /for=d: /on=d: /maxsize=unbounded |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 159809, Reason: Child Process |
| Unmonitor End Time | End Time: 161699, Reason: Terminated |
| Monitor duration | 1.89s |
| Return Code | 2 |
| PID | 4696 |
| Parent PID | 3640 |
| Bitness | 32 Bit |

### Process #14: vssadmin.exe

| | |
|---|---|
| ID | 14 |
| File Name | c:\windows\syswow64\vssadmin.exe |
| Command Line | vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 162011, Reason: Child Process |
| Unmonitor End Time | End Time: 165213, Reason: Terminated |
| Monitor duration | 3.20s |
| Return Code | 2 |
| PID | 1616 |
| Parent PID | 3640 |
| Bitness | 32 Bit |

### Process #15: vssadmin.exe

| | |
|---|---|
| ID | 15 |
| File Name | c:\windows\syswow64\vssadmin.exe |
| Command Line | vssadmin resize shadowstorage /for=e: /on=e: /maxsize=unbounded |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 165831, Reason: Child Process |
| Unmonitor End Time | End Time: 168968, Reason: Terminated |
| Monitor duration | 3.14s |
| Return Code | 2 |
| PID | 5088 |
| Parent PID | 3640 |
| Bitness | 32 Bit |

### Process #16: vssadmin.exe

| | |
|---|---|
| ID | 16 |
| File Name | c:\windows\syswow64\vssadmin.exe |
| Command Line | vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 168969, Reason: Child Process |
| Unmonitor End Time | End Time: 171517, Reason: Terminated |
| Monitor duration | 2.55s |
| Return Code | 2 |
| PID | 4648 |
| Parent PID | 3640 |
| Bitness | 32 Bit |

### Process #17: vssadmin.exe

| | |
|---|---|
| ID | 17 |
| File Name | c:\windows\syswow64\vssadmin.exe |
| Command Line | vssadmin resize shadowstorage /for=f: /on=f: /maxsize=unbounded |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 172045, Reason: Child Process |
| Unmonitor End Time | End Time: 174620, Reason: Terminated |
| Monitor duration | 2.58s |
| Return Code | 2 |
| PID | 1284 |
| Parent PID | 3640 |
| Bitness | 32 Bit |

### Process #18: vssadmin.exe

| | |
|---|---|
| ID | 18 |
| File Name | c:\windows\syswow64\vssadmin.exe |
| Command Line | vssadmin resize shadowstorage /for=g: /on=g: /maxsize=401MB |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 174725, Reason: Child Process |
| Unmonitor End Time | End Time: 175592, Reason: Terminated |
| Monitor duration | 0.87s |
| Return Code | 2 |
| PID | 2128 |
| Parent PID | 3640 |
| Bitness | 32 Bit |

### Process #19: vssadmin.exe

| | |
|---|---|
| ID | 19 |
| File Name | c:\windows\syswow64\vssadmin.exe |
| Command Line | vssadmin resize shadowstorage /for=g: /on=g: /maxsize=unbounded |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 175593, Reason: Child Process |
| Unmonitor End Time | End Time: 176906, Reason: Terminated |
| Monitor duration | 1.31s |
| Return Code | 2 |
| PID | 4824 |
| Parent PID | 3640 |
| Bitness | 32 Bit |

### Process #20: vssadmin.exe

| | |
|---|---|
| ID | 20 |
| File Name | c:\windows\syswow64\vssadmin.exe |
| Command Line | vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 176733, Reason: Child Process |
| Unmonitor End Time | End Time: 178547, Reason: Terminated |
| Monitor duration | 1.81s |
| Return Code | 2 |
| PID | 3984 |
| Parent PID | 3640 |
| Bitness | 32 Bit |

### Process #21: vssadmin.exe

| | |
|---|---|
| ID | 21 |
| File Name | c:\windows\syswow64\vssadmin.exe |
| Command Line | vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 178090, Reason: Child Process |
| Unmonitor End Time | End Time: 181307, Reason: Terminated |
| Monitor duration | 3.22s |
| Return Code | 2 |
| PID | 952 |
| Parent PID | 3640 |
| Bitness | 32 Bit |

### Process #22: vssadmin.exe

| | |
|---|---|
| ID | 22 |
| File Name | c:\windows\syswow64\vssadmin.exe |
| Command Line | vssadmin Delete Shadows /all /quiet |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 181595, Reason: Child Process |
| Unmonitor End Time | End Time: 183964, Reason: Terminated |
| Monitor duration | 2.37s |
| Return Code | 2 |
| PID | 2920 |
| Parent PID | 3640 |
| Bitness | 32 Bit |

# ARTIFACTS

## File

| SHA256 | File Names | Category | File Size | MIME Type | Operations | Verdict |
|---|---|---|---|---|---|---|
| be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8 | C:\Users\RDhJ0CNFevzX\Desktop\be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe, \??\C:\Users\RDhJ0CNFevzX\Desktop\be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe | Sample File | 221.00 KB | application/vnd.microsoft.portable-executable | Access, Delete | MALICIOUS |
| 8940135a58d28338ce4ea9b9933e6780507c56ab37a2f2e3a1a98c6564548a12 | C:\Users\Public\sys.bat | Dropped File | 1.48 KB | text/plain | Access, Create, Read, Write | MALICIOUS |
| 75f25a3c2d1383ff052b7848e1133c383075e8f65b8a70eb2fd49321dcf076b0 | C:\ProgramData\newpatek\onmywrist.bat, \??\C:\ProgramData\newpatek\onmywrist.bat | Dropped File | 346 bytes | text/x-msdos-batch | Access, Create, Read, Write | CLEAN |
| fa7943a3aed783cd7ed4c6e95be582876c1f02c2120472 1d216eff2597962cdb | C:\Program Files\Common Files\microsoft shared\ClickToRun\ServiceWatcherSchedule.xml[newpatek@cock.li].MARRA | Dropped File | 4.61 KB | application/octet-stream | Access, Create, Read, Write | CLEAN |
| 75ceb6d60b0abf24795bd77de0fc9b8f9958638bf111f04e831714a34b3beb47 | C:\Users\Public\MARRACRYPT_ID_DO_NOT_TOUCH | Dropped File | 1.66 KB | application/octet-stream | Access, Create, Read, Write | CLEAN |
| cc1d60af1cc96282afa832d3f65cacbcc612c47e00d2006beb5949b144d1638e | C:\Users\Public\PUBLIC_KEY_DO_NOT_TOUCH | Dropped File | 276 bytes | application/octet-stream | Access, Create, Write | CLEAN |
| 6e110d252e956412713fcc9b7fa0cb6b195a6d6626516356 29e44a7d101e0b52 | C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeUpdateSchedule.xml[newpatek@cock.li].MARRA | Dropped File | 4.94 KB | application/octet-stream | Access, Create, Read, Write | CLEAN |
| ab87b945b4cd562202394bf73e6fd2f604a6ffdb3b31307418ba47d9b8cfd7b3 | C:\Program Files\Common Files\n_NxG3TG8VT.jpg[newpatek@cock.li].MARRA | Dropped File | 25.58 KB | application/octet-stream | Access, Create, Read, Write | CLEAN |
| 037632396b47ec22658e15758a6a1b7357b1a39703f8eafe9e0cf6bc0bc0024d | C:\Program Files\Common Files\microsoft shared\ClickToRun\C2RHeartbeatConfig.xml[newpatek@cock.li].MARRA | Dropped File | 4.31 KB | application/octet-stream | Access, Create, Read, Write | CLEAN |
| b8c94f3f2f59902accf583a1d63607d4edd6b74f32ff46d6562fd9774e472997 | C:\Users\Public\MARRACRYPT_ID_DO_NOT_TOUCH | Dropped File | 1.14 KB | application/octet-stream | Access, Create, Read, Write | CLEAN |
| 88f0015ad381b66e803842931dda2704b5d0076392f69b66e8a964e222e3cc8d | C:\Boot\MARRACRYPT_INFORMATION.HTML, C:\Program Files\Common Files\microsoft shared\ink\ja-JP\MARRACRYPT_INFORMATION.HTML, C:\Prog... ...shared\ink\bg-BG\MARRACRYPT_INFORMATION.HTML, C:\Program Files\Common Files\microsoft shared\ink\en-US\MARRACRYPT_INFORMATION.HTML | Dropped File | 6.24 KB | text/html | Access, Create, Write | CLEAN |

## Filename

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| C:\Users\RDhJ0CNFevzX\Desktop\be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe | Sample File, Accessed File, VM File | Access, Delete | MALICIOUS |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\HxCalendarBadge.scale-150.png | Accessed File | Access | CLEAN |
| \??\c:\Users\RDhJ0CNFevzX\AppData\Local\Packages\windows.immersivecontrolpanel_cw5n1h2txyewy\LocalState\Indexed\Settings\en-US\AAA_SystemSettings_Language_Installed_Profiles_Collection.settingcontent-ms | Accessed File | Access, Write | CLEAN |

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| C:\Program Files\WindowsApps\Microsoft.Office.Sway_17.6216.20251.0_x64__8wekyb3d8bbwe\images\6478_40x40x32.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.3DBuilder_10.9.50.0_x64__8wekyb3d8bbwe\Assets\LightBlue.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.CommsPhone_1.10.15000.0_x64__8wekyb3d8bbwe\Assets\BaseVoicemail2MedTileThin.scale-200.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsMaps_4.1509.50911.0_x64__8wekyb3d8bbwe\Assets\Images\ShareGlyphs\glyph_0xea22.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Getstarted_2.3.7.0_x64__8wekyb3d8bbwe\Content\desktop\MARRACRYPT_INFORMATION.HTML | Accessed File | Access, Create | CLEAN |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\5511_20x20x32.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.Sway_17.6216.20251.0_x64__8wekyb3d8bbwe\images\contrast-white\SwayAppList.targetsize-48.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\Common Files\microsoft shared\ink\fsdefinitions\main\zh-changjei.xml[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Getstarted_2.3.7.0_x64__8wekyb3d8bbwe\Assets\GetStartedAppList.targetsize-48_altform-unplated_contrast-white.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.MicrosoftSolitaireCollection_3.3.9211.0_neutral_split.scale-100_8wekyb3d8bbwe\Assets\Awards\challenge\Came_To_Win_Unearned_small.scale-100.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\videos\OneNoteFRE_ClipAndAdd_LTR_Tablet.mp4[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsCamera_2015.1071.40.0_x64__8wekyb3d8bbwe\Assets\WindowsIcons\WindowsCameraWideTile.contrast-black_scale-200.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.People_10.0.2840.0_x64__8wekyb3d8bbwe\Assets\contrast-black\PeopleAppList.targetsize-96.png | Accessed File | Access | CLEAN |
| C:\Program Files\Windows Multimedia Platform\MARRACRYPT_INFORMATION.HTML | Dropped File, Accessed File | Access, Create, Write | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.Sway_17.6216.20251.0_x64__8wekyb3d8bbwe\images\5313_40x40x32.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\contrast-white\HxCalendarAppList.targetsize-60.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.Sway_17.6216.20251.0_x64__8wekyb3d8bbwe\images\8498_40x40x32.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\HxMailAppList.targetsize-36_altform-unplated.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\contrast-white\HxMailBadge.scale-100.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\images\PageGalleryViewBackground.png | Accessed File | Access | CLEAN |

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| C:\Program Files\WindowsApps\Microsoft.WindowsCamera_2015.1071.40.0_x64__8wekyb3d8bbwe\Assets\WindowsIcons\WindowsCameraAppList.contrast-white_targetsize-30.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\images\contrast-white\OneNotePageMedTile.scale-125.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\Common Files\System\ado\msado60.tlb | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.MicrosoftSolitaireCollection_3.3.9211.0_x64__8wekyb3d8bbwe\Assets\HowToPlay\FreeCell\Control_1.jpg | Accessed File | Access | CLEAN |
| \??\c:\Users\RDhJ0CNFevzX\AppData\Local\Packages\windows.immersivecontrolpanel_cw5n1h2txyewy\LocalState\Indexed\Settings\en-US\AAA_SystemSettings_Input_Touch_PanEnabled.settingcontent-ms | Accessed File | Access, Write | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsPhone_10.1510.9010.0_x64__8wekyb3d8bbwe\html\lv-lv\offline.xhtml | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.BingSports_4.6.169.0_x86__8wekyb3d8bbwe\Assets\AppTiles\contrast-white\Sports_TileLargeSquare.scale-100.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.CommsPhone_1.10.15000.0_x64__8wekyb3d8bbwe\Assets\MissedCall.targetsize-24.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsAlarms_10.1510.12020.0_x64__8wekyb3d8bbwe\Assets\AlarmsAppList.contrast-black_targetsize-60.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\images\contrast-white\OneNoteNotebookWideTile.scale-125.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\images\contrast-black\OneNoteSectionLargeTile.scale-150.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.Sway_17.6216.20251.0_x64__8wekyb3d8bbwe\images\8041_40x40x32.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\HxMailAppList.targetsize-32_altform-unplated.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\bg3_thumb.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsAlarms_10.1510.12020.0_x64__8wekyb3d8bbwe\Assets\WorldClockWideTile.contrast-white_scale-200.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Windows.Photos_15.1001.16470.0_x64__8wekyb3d8bbwe\Bing.Immersive\Shaders\SimpleCubeShader-downlevel.ps | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\images\contrast-white\OneNoteSmallTile.scale-200.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\5372_32x32x32.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\2708_32x32x32.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| C:\Program Files\WindowsApps\Microsoft.MicrosoftSolitaireCollection_3.3.9211.0_x64__8wekyb3d8bbwe\Assets\DailyChallenges\SmallSpiderTile.jpg | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.VCLibs.140.00_14.0.22929.0_x86__8wekyb3d8bbwe\logo.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.Sway_17.6216.20251.0_x64__8wekyb3d8bbwe\images\SwayWideLogo.scale-100.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\images\contrast-black\OneNoteSectionGroupLargeTile.scale-150.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.Sway_17.6216.20251.0_x64__8wekyb3d8bbwe\images\SwayAppList.targetsize-16.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsCalculator_10.1510.9020.0_x64__8wekyb3d8bbwe\Assets\CalculatorAppList.contrast-white_targetsize-80.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\images\1851_20x20x32.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsCalculator_10.1510.9020.0_neutral_split.scale-100_8wekyb3d8bbwe\Assets\CalculatorWideTile.contrast-black_scale-100.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Windows\SYSTEM32\psapi.dll | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsCamera_2015.1071.40.0_x64__8wekyb3d8bbwe\Assets\WindowsIcons\WindowsCameraAppList.targetsize-48.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\1914_32x32x32.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsCalculator_10.1510.9020.0_neutral_split.scale-100_8wekyb3d8bbwe\Assets\CalculatorWideTile.contrast-white_scale-100.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.Sway_17.6216.20251.0_x64__8wekyb3d8bbwe\images\7656_48x48x32.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.Sway_17.6216.20251.0_x64__8wekyb3d8bbwe\Assets\WebPlayer\storypageeditcommon.js | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Windows.Photos_15.1001.16470.0_x64__8wekyb3d8bbwe\Assets\PhotosAppList.targetsize-20.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\Internet Explorer\en-US\MARRACRYPT_INFORMATION.HTML | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\SwipeTeachingCalloutArchiveImage.layoutdir-LTR.gif | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\wordxaml\view\controls\navindicatorcontrol.xbf | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsMaps_4.1509.50911.0_x64__8wekyb3d8bbwe\Assets\AppTiles\contrast-white\MapsAppList.targetsize-32.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.Sway_17.6216.20251.0_x64__8wekyb3d8bbwe\images\offsymsb.ttf | Accessed File | Access | CLEAN |

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\5372_40x40x32.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.NET.Native.Runtime.1.0_1.0.22929.0_x64__8wekyb3d8bbwe\AppxSignature.p7x | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\6021_20x20x32.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.BingWeather_4.6.169.0_neutral_~_8wekyb3d8bbwe\AppxSignature.p7x | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.MicrosoftSolitaireCollection_3.3.9211.0_x64__8wekyb3d8bbwe\Assets\DailyChallenges\Icons\klondike.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsAlarms_10.1510.12020.0_neutral_split.scale-100_8wekyb3d8bbwe\Assets\StopwatchSmallTile.scale-100.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\images\contrast-black\OneNoteAppList.targetsize-36_altform-unplated.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.MicrosoftSolitaireCollection_3.3.9211.0_x64__8wekyb3d8bbwe\Assets\backgroundTile.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.MicrosoftSolitaireCollection_3.3.9211.0_x64__8wekyb3d8bbwe\Assets\OptInPopup\MARRACRYPT_INFORMATION.HTML | Accessed File | Access, Create | CLEAN |
| C:\Windows\SYSTEM32\bcrypt.dll | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Messaging_1.10.22012.0_x86__8wekyb3d8bbwe\Assets\SkypeLine\SkypeOSSAttributions.htm[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.MicrosoftSolitaireCollection_3.3.9211.0_neutral_split.scale-100_8wekyb3d8bbwe\Assets\Awards\spider\2_Piece_Silk_Suit_.scale-100.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\5313_20x20x32.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.MicrosoftOfficeHub_17.6306.23501.0_x64__8wekyb3d8bbwe\images\1937_20x20x32.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsCalculator_10.1510.9020.0_neutral_split.scale-100_8wekyb3d8bbwe\Assets\CalculatorMedTile.contrast-black_scale-100.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Windows.Photos_15.1001.16470.0_x64__8wekyb3d8bbwe\Assets\PhotosAppList.targetsize-40_altform-unplated.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsMaps_4.1509.50911.0_x64__8wekyb3d8bbwe\Assets\SecondaryTiles\Directions\Walking\contrast-white\WalkingWideTile.scale-200.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.MicrosoftSolitaireCollection_3.3.9211.0_neutral_split.scale-100_8wekyb3d8bbwe\Assets\Awards\tripeaks\Expedition_Leader_.scale-100.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\images\contrast-white\OneNotePageMedTile.scale-150.png | Accessed File | Access | CLEAN |

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| C:\Program Files\WindowsApps\Microsoft.WindowsCalculator_10.1510.9020.0_x64__8wekyb3d8bbwe\Assets\CalculatorAppList.targetsize-40_altform-unplated_contrast-black.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\2033_40x40x32.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsMaps_4.1509.50911.0_neutral_split.scale-100_8wekyb3d8bbwe\Assets\SecondaryTiles\Directions\Transit\TransitWideTile.scale-100.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsCamera_2015.1071.40.0_neutral_split.scale-100_8wekyb3d8bbwe\Assets\WindowsIcons\WindowsCameraAppList.contrast-black_scale-100.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\images\7989_32x32x32.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\images\OneNoteSmallTile.scale-125.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsMaps_4.1509.50911.0_x64__8wekyb3d8bbwe\Assets\AppTiles\contrast-white\MapsAppList.targetsize-16.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.MicrosoftOfficeHub_17.6306.23501.0_x64__8wekyb3d8bbwe\images\6478_40x40x32.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Windows.Photos_15.1001.16470.0_neutral_split.scale-100_8wekyb3d8bbwe\resources.pri | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.BingNews_4.6.169.0_x86__8wekyb3d8bbwe\Microsoft.Advertising\MARRACRYPT_INFORMATION.HTML | Accessed File | Access, Create | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\AppxBlockMap.xml[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsMaps_4.1509.50911.0_x64__8wekyb3d8bbwe\Assets\SecondaryTiles\Places\MapsPinnedPlaceWideTile.scale-200.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.BingWeather_4.6.169.0_x86__8wekyb3d8bbwe\Microsoft.Advertising.winmd | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\images\4654_32x32x32.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsCalculator_10.1510.9020.0_neutral_split.scale-100_8wekyb3d8bbwe\Assets\CalculatorLargeTile.contrast-black_scale-100.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\5313_20x20x32.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsCamera_2015.1071.40.0_x64__8wekyb3d8bbwe\Assets\WindowsIcons\WindowsCameraAppList.contrast-white_targetsize-64.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsMaps_4.1509.50911.0_x64__8wekyb3d8bbwe\Assets\SecondaryTiles\Directions\Transit\TransitLargeTile.scale-200.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\images\rightIcon.png | Accessed File | Access | CLEAN |

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| C:\Program Files\WindowsApps\Microsoft.WindowsMaps_4.1509.50911.0_neutral_split.scale-100_8wekyb3d8bbwe\Assets\AppTiles\contrast-white\MapsWideTile.scale-100.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\Common Files\microsoft shared\ink\en-US\correct.avi | Accessed File | Access | CLEAN |
| C:\Program Files\Common Files\microsoft shared\ink\ipshi.xml[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\images\icon-snap-menu.scale-180.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\images\5311_40x40x32.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\images\contrast-black\OneNoteSectionSmallTile.scale-200.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.Sway_17.6216.20251.0_x64__8wekyb3d8bbwe\images\1849_20x20x32.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Messaging_1.10.22012.0_neutral_split.scale-150_8wekyb3d8bbwe\Assets\starttile.dualsim1.surprise.scale-150.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.BingFinance_4.6.169.0_x86__8wekyb3d8bbwe\Configuration\configuration.sqlite[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\images\contrast-black\OneNoteSectionLargeTile.scale-125.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\Office365LogoWLockup.scale-100.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.Sway_17.6216.20251.0_x64__8wekyb3d8bbwe\images\7260_48x48x32.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\images\OneNoteNotebookWideTile.scale-400.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.BingFinance_4.6.169.0_x86__8wekyb3d8bbwe\Assets\AppTiles\contrast-black\Money_LogoSmall.targetsize-24.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.CommsPhone_1.10.15000.0_x64__8wekyb3d8bbwe\Assets\MissedCall1.targetsize-16.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.MicrosoftSolitaireCollection_3.3.9211.0_neutral_split.scale-100_8wekyb3d8bbwe\Assets\Icons\friends_activity.scale-100.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\HxMailWideTile.scale-150.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.MicrosoftSolitaireCollection_3.3.9211.0_x64__8wekyb3d8bbwe\Assets\GamePlayAssets\Localization\localized_UK-UA.respack | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.Sway_17.6216.20251.0_x64__8wekyb3d8bbwe\images\contrast-black\SwayMediumLogo.scale-200.png | Accessed File | Access | CLEAN |

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| C:\Program Files\WindowsApps\Microsoft.Messaging_1.10.22012.0_x86__8wekyb3d8bbwe\SkypeApp\Assets\SkypeVideoCallWideTile.scale-150_contrast-white.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Windows.Photos_15.1001.16470.0_x64__8wekyb3d8bbwe\Assets\PhotosSmallTile.contrast-white_scale-100.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsCamera_2015.1071.40.0_x64__8wekyb3d8bbwe\AppxMetadata\MARRACRYPT_INFORMATION.HTML | Accessed File | Access, Create | CLEAN |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\contrast-white\HxMailLargeTile.scale-400.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsCalculator_10.1510.9020.0_x64__8wekyb3d8bbwe\Assets\CalculatorAppList.contrast-black_scale-200.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.Sway_17.6216.20251.0_x64__8wekyb3d8bbwe\Assets\WebPlayer\document_24x24.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\contrast-white\HxMailAppList.scale-100.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\contrast-black\HxMailSplashLogo.scale-100.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsCamera_2015.1071.40.0_x64__8wekyb3d8bbwe\Assets\WindowsIcons\WindowsCameraAppList.contrast-white_targetsize-80.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.Sway_17.6216.20251.0_x64__8wekyb3d8bbwe\images\DoneHero.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.SkypeApp_3.2.1.0_x86__kzf8qxf38zg5c\GetSkype\Assets\SkypeMedTile.scale-100.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsCalculator_2015.1009.20.0_neutral_~_8wekyb3d8bbwe\MARRACRYPT_INFORMATION.HTML | Accessed File | Access, Create | CLEAN |
| C:\Program Files\Common Files\microsoft shared\Stationery\grid_(cm).wmf | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.CommsPhone_1.10.15000.0_x64__8wekyb3d8bbwe\WindowsPhoneReservedAppInfo.xml[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsMaps_4.1509.50911.0_x64__8wekyb3d8bbwe\Assets\AppTiles\contrast-black\MapsAppList.targetsize-30_altform-unplated.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.MicrosoftOfficeHub_17.6306.23501.0_x64__8wekyb3d8bbwe\images\1850_24x24x32.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.3DBuilder_10.9.50.0_x64__8wekyb3d8bbwe\Assets\Contrast\Wide310x150Logo.scale-100.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\HxMailAppList.targetsize-36_altform-colorize.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsMaps_4.1509.50911.0_x64__8wekyb3d8bbwe\Assets\AppTiles\contrast-white\MapsAppList.targetsize-96.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\videos\OneNoteFRE_ClipAndAdd_LTR_Tablet.mp4 | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Messaging_1.10.22012.0_x86__8wekyb3d8bbwe\SkypeApp\Assets\SkypeVideoCallLargeTile.scale-400_contrast-black.png | Accessed File | Access | CLEAN |
| C:\Program Files\Common Files\microsoft shared\ink\ipsplk.xml | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Messaging_1.10.22012.0_x86__8wekyb3d8bbwe\SkypeApp\Assets\SkypeVideoCallLargeTile.scale-200.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.MicrosoftOfficeHub_17.6306.23501.0_x64__8wekyb3d8bbwe\images\7260_32x32x32.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.MicrosoftSolitaireCollection_3.3.9211.0_x64__8wekyb3d8bbwe\Assets\sticker.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\xaml\onenote\OptInCustomizeUI.xaml | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsMaps_4.1509.50911.0_x64__8wekyb3d8bbwe\Assets\AppTiles\contrast-black\MapsAppList.targetsize-40_altform-unplated.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.Office.OneNote_17.6131.10051.0_x64__8wekyb3d8bbwe\xaml\onenote\ShareErrorMessagePage.xaml | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.6308.42271.0_x64__8wekyb3d8bbwe\images\HxCalendarAppList.targetsize-80_altform-fullcolor.png | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsCamera_2015.1071.40.0_x64__8wekyb3d8bbwe\Assets\Square44x44Logo.scale-200.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |
| C:\Program Files\WindowsApps\Microsoft.WindowsCalculator_10.1510.9020.0_neutral_split.scale-100_8wekyb3d8bbwe\Assets\CalculatorStoreLogo.contrast-white_scale-100.png[newpatek@cock.li].MARRA | Accessed File | Access | CLEAN |

## Reduced dataset

### URL

| URL | Category | IP Address | Country | HTTP Methods | Verdict |
|---|---|---|---|---|---|
| https://www.bestbitcoinexchange.io | - | - | - | - | CLEAN |

### Domain

| Domain | IP Address | Country | Protocols | Verdict |
|---|---|---|---|---|
| www.bestbitcoinexchange.io | - | - | - | CLEAN |

### Registry

| Registry Key | Operations | Parent Process Name | Verdict |
|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar | read, access | cmd.exe | CLEAN |
| HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor | read, access | cmd.exe | CLEAN |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion | read, access | cmd.exe | CLEAN |
| HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System | access | cmd.exe | CLEAN |
| HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun | read, access | cmd.exe | CLEAN |

| Registry Key | Operations | Parent Process Name | Verdict |
|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion | read, access | cmd.exe | CLEAN |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun | read, access | cmd.exe | CLEAN |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions | read, access | cmd.exe | CLEAN |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar | read, access | cmd.exe | CLEAN |
| HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck | read, access | cmd.exe | CLEAN |
| HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions | read, access | cmd.exe | CLEAN |
| HKEY_CURRENT_USER\Software\Microsoft\Command Processor | access | cmd.exe | CLEAN |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar | read, access | cmd.exe | CLEAN |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor | access | cmd.exe | CLEAN |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor | read, access | cmd.exe | CLEAN |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DisableUNCCheck | read, access | cmd.exe | CLEAN |
| HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar | read, access | cmd.exe | CLEAN |

## Process

| Process Name | Commandline | Verdict |
|---|---|---|
| be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe | "C:\Users\RDhJ0CNFevzX\Desktop\be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe" | MALICIOUS |
| cmd.exe | "cmd.exe" /C "C:\Users\Public\sys.bat" | SUSPICIOUS |
| cmd.exe | C:\Windows\system32\cmd.exe /c ""C:\ProgramData\newpatek\onmywrist.bat"" | SUSPICIOUS |
| vssadmin.exe | vssadmin Delete Shadows /all /quiet | CLEAN |
| cmd.exe | C:\Windows\system32\cmd.exe /c tasklist /NH /FI "IMAGENAME eq be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe" | CLEAN |
| tasklist.exe | tasklist /NH /FI "IMAGENAME eq be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe" | CLEAN |
| vssadmin.exe | vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB | CLEAN |
| vssadmin.exe | vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded | CLEAN |
| vssadmin.exe | vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB | CLEAN |
| vssadmin.exe | vssadmin resize shadowstorage /for=d: /on=d: /maxsize=unbounded | CLEAN |
| vssadmin.exe | vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB | CLEAN |
| vssadmin.exe | vssadmin resize shadowstorage /for=e: /on=e: /maxsize=unbounded | CLEAN |
| vssadmin.exe | vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB | CLEAN |
| vssadmin.exe | vssadmin resize shadowstorage /for=f: /on=f: /maxsize=unbounded | CLEAN |
| vssadmin.exe | vssadmin resize shadowstorage /for=g: /on=g: /maxsize=401MB | CLEAN |
| vssadmin.exe | vssadmin resize shadowstorage /for=g: /on=g: /maxsize=unbounded | CLEAN |
| vssadmin.exe | vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB | CLEAN |
| vssadmin.exe | vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded | CLEAN |

| Process Name | Commandline | Verdict |
| --- | --- | --- |
| vssadmin.exe | vssadmin Delete Shadows /all /quiet | CLEAN |

## YARA / AV

### YARA (3)

| Ruleset Name | Rule Name | Rule Description | File Type | File Name | Classification | Verdict |
|---|---|---|---|---|---|---|
| Generic | Packer_RedNet | Packer used to distribute malware | Memory Dump | - | - | 5/5 |
| Generic | Packer_RedNet | Packer used to distribute malware | Memory Dump | - | - | 5/5 |
| Generic | Packer_RedNet | Packer used to distribute malware | Sample File | C:\Users\RDhJ0CNFevzX\Desktop\be88512c9250a558a3524e1c3bbd0299517cb0d6c3fb749c22df32033bf081e8.exe | - | 5/5 |

# ENVIRONMENT

### Virtual Machine Information

| | |
|---|---|
| Name | win10_64_th2_en_mso2016 |
| Description | win10_64_th2_en_mso2016 |
| Architecture | x86 64-bit |
| Operating System | Windows 10 Threshold 2 |
| Kernel Version | 10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379) |
| Network Scheme Name | Local Gateway |
| Network Config Name | Local Gateway |

### Platform Information

| | |
|---|---|
| Platform Version | 4.5.0 |
| Dynamic Engine Version | 4.5.0 / 04/22/2022 19:04 |
| Static Engine Version | 4.5.0.0 / 2022-04-22 17:45:13 |
| AV Exceptions Version | 4.5.0.2 / 2022-04-03 15:57:54 |
| Link Detonation Heuristics Version | 4.5.0.19 / 2022-04-20 05:46:11 |
| Smart Memory Dumping Rules Version | 4.5.0.2 / 2022-04-03 15:57:54 |
| Config Extractors Version | 4.5.0.14 / 2022-04-07 17:00:08 |
| Signature Trust Store Version | 4.5.0.2 / 2022-04-03 15:57:54 |
| VMRay Threat Identifiers Version | 4.5.0.24 / 2022-04-26 09:10:00 |
| YARA Built-in Ruleset Version | 4.5.0.2 |

### Software Information

| | |
|---|---|
| Adobe Acrobat Reader Version | Not installed |
| Microsoft Office | 2016 |
| Microsoft Office Version | 16.0.4266.1003 |
| Hangul Office | Not installed |
| Hangul Office Version | Not installed |
| Internet Explorer Version | 11.0.10586.0 |
| Chrome Version | Not installed |
| Firefox Version | Not installed |
| Flash Version | Not installed |
| Java Version | Not installed |

### System Information

| | |
|---|---|
| Sample Directory | C:\Users\RDhJ0CNFevzX\Desktop |
| Computer Name | XC64ZB |
| User Domain | XC64ZB |
| User Name | RDhJ0CNFevzX |
| User Profile | C:\Users\RDhJ0CNFevzX |
| Temp Directory | C:\Users\RDHJ0C~1\AppData\Local\Temp |

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