SHA256	52765525103f5b3b07d0882cc8ee4bb8e279ad5d451e1ed07cae3b98565cce29
SHA512	082594fced158d5597e1b34ec220fd873365f3ec282add680fc84d4b31010c2485e97611049c2d1432b6a1014784e06d3b11f14a815252a28c0c38c4eb5a31e1
ssdeep	96:XaMTeYZR1Bm3AboPwVUJyWvihHbP11Ho+5EGsW7MlDz1v7Yrtgx3X:XaWZZR1Bx9VP16+5jRQlDR8U
Entropy	7.963703

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

5276552510...	Used_By	d221ca9c519ae04c7724baca8d36c2ce77454e0f9aa0f119ecfa9246973a92f8

Description

This artifact is the encrypted configuration file for the OneDriveClient module contained in the file Uploader.exe (d221ca9c519ae04c7724baca8d36c2ce77454e0f9aa0f119ecfa9246973a92f8) detailed in this report. The data is decrypted using the hard-coded AES-256-CBC key 'M(xcHq88q[s=pc7^+u_Gb_}JC%QQwP:h'. The algorithm uses an IV that is derived from the first half of the encryption key (See Figure 8 above).

The file contains multiple paths to archives targeted by the attacker. The file includes the IP address of the server, stolen credential information, and a key to encrypt the uploaded data. NOTE: The decrypted configuration contains confidential client information and therefore is not included in this report.

In addition, the data contains a refresh token for an OAuth client for Microsoft Azure with the Client ID of '7a3b4b84-ed28-4f18-b30d-218788c74a5f'. Speed and compression information as well as times that the OneDrive share can be accessed are also included in the configuration.

09605981a072c604e6ef9ad2dd7d2a78b48b07ee3339589bfcf0a466a9190904

Details

Name	msexch.log
Size	103904 bytes
Type	data
MD5	30ea2a37c7174ed8c3ab88aecee0002b
SHA1	3a6f2826aab7948d8b930f6bf13897160c198807
SHA256	09605981a072c604e6ef9ad2dd7d2a78b48b07ee3339589bfcf0a466a9190904
SHA512	0a78caf6257b8b58578181a9555bf9cee24b1bfced078855145f79757701a53a15968d9bb6acc74fdc9469bd28fa82a53b8d52669fa3952824f51339bd94ad7a
ssdeep	3072:OcopRvQlpMV/EN6PmW9tV/PUdpogFeSQx7:CpVFp8/pFhPUdponR7
Entropy	7.998490

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

09605981a0...	Created_By	d221ca9c519ae04c7724baca8d36c2ce77454 e0f9aa0f119ecfa9246973a92f8

Description

This artifact is a log file created by the OneDriveClient.UploadedFiles function contained in the file Uploader.exe (d221ca9c519ae04c7724baca8d36c2ce77454e0f9aa0f119ecfa9246973a92f8). The file contains the MD5 hash of each file that has been uploaded to the remote server.

6a0cd866c849e62f9ccc26575d8794c2e0b14722387742b965d4358e1e0e8b3c

Details

Name	msexch_temp.log
Size	103904 bytes
Type	data
MD5	20b7eb0af9b9e7403a298f7966d5a1d4
SHA1	b2018e61e8b435b6a172b35774377ebc16fd0168
SHA256	6a0cd866c849e62f9ccc26575d8794c2e0b14722387742b965d4358e1e0e8b3c
SHA512	3695120b452c103f54c4eb738648621f162850ec32aca734ecdd552755ecced1500aaf789ec1bf45afc5df4fcfd6144ca4d1fff415a25656dd5493f81b221bfe
ssdeep	3072:2H05Z4/LivIjqjSXZa8HaDhpfUcJkm0YK/:29ivImjSX9qnUcdi
Entropy	7.998385

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

6a0cd866c8...	Created_By	d221ca9c519ae04c7724baca8d36c2ce77454 e0f9aa0f119ecfa9246973a92f8

Description

This artifact is a log file created by the OneDriveClient.UploadedFiles function contained in the file Uploader.exe (d221ca9c519ae04c7724baca8d36c2ce77454e0f9aa0f119ecfa9246973a92f8). The file contains the MD5 hash of the path for each file that has been uploaded to the remote server.

---

fae38156e9ce12368c846836b87861f4f12e14698cb65f14545205fa56d8c496

Tags

information-stealer

Details

Name	vmware.ps1
Size	10436 bytes
Type	ASCII text
MD5	4825b1e32ff062f4671d5420661695af
SHA1	0cbf85f88e2fb0bc721357acdd543d5a1957886f
SHA256	fae38156e9ce12368c846836b87861f4f12e14698cb65f14545205fa56d8c496
SHA512	a58298346cdf35e432d755942ef2690c6e3182a4fab03df163142e42cdcb0d7bc3810c647078a779d15ee0676b0eacfa59c38512671dc86264b42f2c8d69edb8

ssdeep	192:k9XNMA6GyvE0XJvP0EN3ab3Akz9JUWCUVCRB7/dUV /TpraVm5efUo9wQUyfa3gpA:k9XNMA6pXJvPCUjUmUvaME8obUaYgpj8
Entropy	4.979828

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Description

This artifact is a script called Export-MFT.ps1 written in PowerShell used to collect the MFT from a system volume. The benign open source script is available on GitHub.

---

bfa7adeda4597b70bf74a9f2032df2f87e07f2dbb46e85cb7c091b83161d6b0a

Details

Name	vmware.exe
Size	497104 bytes
Type	PE32 executable (console) Intel 80386, for MS Windows
MD5	0acb06da48d86e1ef15c27a4f5a3bddd
SHA1	12dd7a86001ff2b6b661cd7de60ca6aadc9b78ae
SHA256	bfa7adeda4597b70bf74a9f2032df2f87e07f2dbb46e85cb7c091b83161d6b0a
SHA512	98fbcd4e190e0bc17dc712bbbe808c7d24610c334925381544fb16a8f75931db1c5f6597cafbe6a12a9050e482e553 51bedb76b40573f8a7489e3c7755bdecd2
ssdeep	12288:1NsUjyDukqiudnJkx3piQLmGLvdnTJ0CRUyF1l3Kl:1mkyDuZiCccQLmGpTrCm1l3g
Entropy	6.459391

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2014-12-02 05:07:13-05:00
Import Hash	1324fa350b5f878451cc28b429b96e9b
Company Name	Alexander Roshal
File Description	Command line RAR
Internal Name	Command line RAR
Legal Copyright	Copyright © Alexander Roshal 1993-2014
Original Filename	None
Product Name	WinRAR
Product Version	5.20.0

PE Sections

MD5	Name	Raw Size	Entropy
98efedab8c1234a79df40e93dc82e136	header	1024	2.635435

0b760a9dbbf12c5d32ca265879aabdb2	.text	410112	6.587893
3874d7a1d17b892215dc07687ac3b75c	.rdata	27136	4.857459
e28ebcc7f9a5e3d463ee9d9de071e085	.data	8192	3.720474
5ad98aabb9c5996ee180a98ff9543866	.rsrc	31232	3.540367
ec534cec214c136ef4552b79103e2eaa	.reloc	14336	5.427399

Packers/Compilers/Cryptors

Microsoft Visual C++ ?.?

Description

This artifact is a benign publicly available version of the Roshal archiver (RAR), version 5.20.0. RAR.exe is used to compress and archive other files.

Relationship Summary

84164e1e80...	Used	91a8b31c126a021f5c156742016acdcca7d83eac4b583bae5d4fd0a85a96813b
84164e1e80...	Created	517faa4a0666ec68842f256f08d987935b6ce9ef64e33f027e084e8f45b9366d
517faa4a06...	Created_By	84164e1e8074c2565d3cd178babd93694ce54811641a77ffdc8d1084dd468afb
91a8b31c12...	Used_By	84164e1e8074c2565d3cd178babd93694ce54811641a77ffdc8d1084dd468afb
157a0ffd18...	Related_To	b03ac5eaf2131060ee381e5e46ebc705d8d617a90cc61fa4918174545b4fbaa6
157a0ffd18...	Dropped	1352dbb093a337eb8db9d0135adbe0542bb7e7163616e4f8962919becab171da
157a0ffd18...	Related_To	0b01f392fa030be1ddd549fb79cf280d2a2c745578a56fedd4cb5e9438ae72cb
b03ac5eaf2...	Related_To	157a0ffd18e05bfd90a4ec108e5458cbde01015e3407b3964732c9d4ceb71656
b03ac5eaf2...	Contains	1352dbb093a337eb8db9d0135adbe0542bb7e7163616e4f8962919becab171da
1352dbb093...	Created	5ba0d0bfda372c1f6aa382a70f4ab8427ec998b680510e208fdf878cfda9afe3
1352dbb093...	Created	0b7d15968d44710b3e7f153c04b5038d03900a6685643bc8efe688c4d5a5deab
1352dbb093...	Used	da267c72f58ec487761de99d0f3bcfd87771a36afc06716053960633a74139df
1352dbb093...	Dropped_By	157a0ffd18e05bfd90a4ec108e5458cbde01015e3407b3964732c9d4ceb71656
1352dbb093...	Created	0b01f392fa030be1ddd549fb79cf280d2a2c745578a56fedd4cb5e9438ae72cb
1352dbb093...	Contained_Within	b03ac5eaf2131060ee381e5e46ebc705d8d617a90cc61fa4918174545b4fbaa6
da267c72f5...	Used_By	1352dbb093a337eb8db9d0135adbe0542bb7e7163616e4f8962919becab171da
0b01f392fa...	Created_By	1352dbb093a337eb8db9d0135adbe0542bb7e7163616e4f8962919becab171da
0b01f392fa...	Related_To	157a0ffd18e05bfd90a4ec108e5458cbde01015e3407b3964732c9d4ceb71656
5ba0d0bfda...	Created_By	1352dbb093a337eb8db9d0135adbe0542bb7e7163616e4f8962919becab171da
0b7d15968d...	Created_By	1352dbb093a337eb8db9d0135adbe0542bb7e7163616e4f8962919becab171da

3585c31366...	Used	25afc6741abfa27f5b50844331772466182ebe3f74bc84f911314d1a68c62cb2
3585c31366...	Created	603e75db59285734cfb5a469e984c4e359e660ccb7836ff9c209aec36931bc2b
25afc6741a...	Used_By	3585c3136686d7d48e53c21be61bb2908d131cf81b826acf578b67bb9d8e9350
603e75db59...	Created_By	3585c3136686d7d48e53c21be61bb2908d131cf81b826acf578b67bb9d8e9350
30191b3bad...	Related_To	e03a2c8a6e81cf62ba7401c598ea1d4635b08bbf9c2fec080b536dde29e6392f
30191b3bad...	Dropped	d221ca9c519ae04c7724baca8d36c2ce77454e0f9aa0f119ecfa9246973a92f8
e03a2c8a6e...	Related_To	30191b3badf3cdbc65d0ffeb68e0f26cef10a41037351b0f562ab52fce7432cc
d221ca9c51...	Used	52765525103f5b3b07d0882cc8ee4bb8e279ad5d451e1ed07cae3b98565cce29
d221ca9c51...	Created	09605981a072c604e6ef9ad2dd7d2a78b48b07ee3339589bfcf0a466a9190904
d221ca9c51...	Created	6a0cd866c849e62f9ccc26575d8794c2e0b14722387742b965d4358e1e0e8b3c
d221ca9c51...	Dropped_By	30191b3badf3cdbc65d0ffeb68e0f26cef10a41037351b0f562ab52fce7432cc
5276552510...	Used_By	d221ca9c519ae04c7724baca8d36c2ce77454e0f9aa0f119ecfa9246973a92f8
09605981a0...	Created_By	d221ca9c519ae04c7724baca8d36c2ce77454e0f9aa0f119ecfa9246973a92f8
6a0cd866c8...	Created_By	d221ca9c519ae04c7724baca8d36c2ce77454e0f9aa0f119ecfa9246973a92f8

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

- 1-888-282-0870
- CISA Service Desk (UNCLASS)
- CISA SIPR (SIPRNET)
- CISA IC (JWICS)

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://us-cert.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.