ANALYSIS REPORT

Malware Analysis Report

10443863.r1.v1 NUMBER

2023-06-15 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

CISA received three files for analysis. The files included three webshells written in PHP: Hypertext Preprocessor (PHP), Active Server Pages Extended (ASPX), and .NET Dynamic-Link Library (DLL). The sample “sd.php” is highly obfuscated and uses rot13 algorithm, zlib for compression and base64 encoding for obfuscation. The “osker.aspx” webshell code was padded with junk code. The .NET DLL webshell is a .NET compiled version of osker.aspx. The samples are interactive webshells and have the ability to upload and manage files, create directories and files, and execute commands on the target machine.

Submitted Files (3)

6ce087b904af8a01aae73ac77d81822ad41799f89a5d301dce45191c897012aa (osker.aspx)

b63c95300c8e36b5e6d3393da12931683796f88fd4601ba8364658b4d12ac05b (App_Web_jl37rjxu.dll)

ea98368f6ecb5281654a6a9e4c649ef9b53860f1ee32340145b61e0e42e1072a (sd.php)

Findings

ea98368f6ecb5281654a6a9e4c649ef9b53860f1ee32340145b61e0e42e1072a

Tags

obfuscated trojan uploader webshell

Details

Name	sd.php
Size	5934 bytes
Type	ASCII text, with very long lines, with CRLF line terminators
MD5	f899d6cbe1be6395a0fa2a802b8eb579
SHA1	e5f29cac0570665bc12f54a7e1894f139cc7b45e
SHA256	ea98368f6ecb5281654a6a9e4c649ef9b53860f1ee32340145b61e0e42e1072a
SHA512	6a9c23c3bd8a4b5f7301b80b7187ed6ae055a4e05e2b817800ddade99cb45e50bf3a96a57f9593aa8dfb49934ea48dba722ba3f4b0e8a8a634e6c86da335dcba
ssdeep	96:8byUcBL9vPh8onLQKwz9UL0wJ0v7R/+B3Oam8WgbVxzbiMhrhRrwSLpVt8lTHGk4:icBL9vFnL1wzGL0tt/cVxzvhrhRZl4hO
Entropy	6.110792

Antivirus

ESET	PHP/Agent.NPM trojan

YARA Rules

- rule CISA_10443863_01 : backdoor remote_access_trojan webshell exploitation information_gathering remote_access accesses_remote_machines anti_debugging captures_system_state_data controls_local_machine compromises_data_availability compromises_data_integrity fingerprints_host installs_other_components
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10443863"
      Date = "2023-05-11"
      Last_Modified = "20230522_1200"
      Actor = "n/a"
      Family = "n/a"
      Capabilities = "accesses-remote-machines anti-debugging captures-system-state-data controls-local-machine compromises-data-availability compromises-data-integrity fingerprints-host installs-other-components"
      Malware_Type = "backdoor remote-access-trojan webshell"
      Tool_Type = "exploitation information-gathering remote-access"
      Description = "Detects obfuscated and deobfuscated interactive PHP webshell samples"
      SHA256 = "ea98368f6ecb5281654a6a9e4c649ef9b53860f1ee32340145b61e0e42e1072a"
    strings:
      $e0 = { 65 76 61 6c }
      $e1 = { 72 6f 74 31 33 }
      $e2 = { 62 61 73 65 36 34 }
      $e3 = { 67 7a 69 6e 66 6c 61 74 65 }
      $e4 = { 73 68 65 6c 6c }
      $e5 = { 78 61 69 73 79 6e 64 69 63 61 74 65 }
      $e6 = { 54 75 62 61 67 75 73 4e 4d }
      $s0 = { 58 30 4d 42 31 33 }
      $s1 = { 74 75 6e 61 66 65 65 73 68 }
      $s2 = { 70 61 73 73 77 6f 72 64 }
      $s3 = { 6f 6e (63 | 43) 6c 69 63 6b 3d }
      $s4 = { 6a 61 76 61 73 63 72 69 70 74 3a 78 79 6e }
    condition:
      (6 of ($e*)) or (3 of ($s*))
  }

ssdeep Matches

No matches found.

Description

This sample is an obfuscated PHP interactive webshell. This webshell is encoded and obfuscated using rot13, gzinflate and base64 as seen in the following code: “eval(str_rot13(gzinflate(str_rot13(base64_decode(($sym))))));” The obfuscated code is a string and is stored in the $sym variable from where it is read and decoded upon execution (Figure 1). The webshell requires the password "pass" for authentication and uses the string “$xyn='tunafeesh';” as a cookie to authenticate.

This webshell enumerates the local system it infects including the operating system, current user, directories, files and permissions. The webshell has the ability to create, rename, and delete files and directories. Furthermore, it has the ability to upload additional files to the affected webserver, run in Safe Mode and execute commands via cmd.exe (Figure 2). The webshell provides a Graphical User Interface (GUI) to the operator to perform these operations on the infected machine.

---Notable Strings Begin---
eval(str_rot13(gzinflate(str_rot13(base64_decode(($sym))))));
tunafeesh
pass
TubagusNM

xaisyndicate
garuda tersakti
con7ext_shell
b374k shell
X0MB13
X0MB13@REBORN.COM
hxxp[:]//www[.]twitter[.]com/X0MB13_
hxxp[:]//www[.]fb[.]com/xombie.xombie.7
onClick="xyn
---Notable Strings End---

Screenshots

```
<br />
<b>Warning</b>:  ob_start(): output handler 'ob_gzhandler' conflicts with 'zlib output
compression' in <b>/home/aravalcl/public_html/wp/wp-content/plugins/seo/alfa-index.php(3) :
eval()'d code(1) : eval()'d code</b> on line <b>3245</b><br />
<?php

/**
Design by TubagusNM
Default pass cgi: xaisyndicate
Thx to con7ext_shell, b374k shell, and all members garuda tersakti 72
**/


@ini_set('output_buffering',0);
@ini_set('display_errors', 0);

$sym = "7Rv9aptT8uf2vf4PG0wN0lLRVJw2SiHI1a7t3l0bO8rHeJ3k8UuygCUVwSI4g6v//XNpAQFPtpy73nSTOHNqdH
N0dHN0c4eFM1OZwbhSmRObq86wq37xbHu+MDXFZFov5NyOFOiKw0F529zptI3jo9Ozaorl2bbyodslNzBH7dS0Nj7MKAtg
GJB8V69w3k6yPUWF7REnQWyn++jw6yHMvSYJaowoQY3Y7EBGWfyAp5az6JSIPnxVHuTsXBwd/
    fRp+g6Jf+gSylWt706JG+TWjJ3YZmBXlQQxl5O0Rq4tPZubHvBvGK/e/jw1jK7atjm74sywduh1euNnbfLn6cm7lvx
6nB69OvvLi5N264PaaRFGsyLLEEJAte27zGOBgLaCFU6DZNMRHZ1hXyFhHIyVPgylC2sUXata1wq7YG2Qv5HSgHjAtQEjH
aXoRSrjnc1m92xUmYTUZ4hCE8rGPotGm5r60beTAWnrV2pcgdAOfD8Mh1D96NWrAgT4nwXIOvxPSZb+9YWmHByKP4raaeY
Otr8Rf9BA2rbjMVRGJpGTJvok4l6gQpzYVrguFsXNq47y5uzs2GsD6kpjwZpB/jq8PB8dQQYSY287C/i1pMGC3Cw9/
    23FqHiiR8T8fVKVWII2zg965PaxHf/Cx99LjnmFXhoni/EZ41jXj7hQLkJ7IH47vuI92zN6AiqIUGgdjQ7MG4vaYA7
UHIfxnAeqUK3xdXXN1YSHjnxl+BxziLyAzsbQJvjzFfwsE+Av4+fg2Tfe4eiZpJne3AvFIzf1Ugn8gPuUbII3k5q8srYLm
```

Figure 1. - $sym variable with obfuscated code.

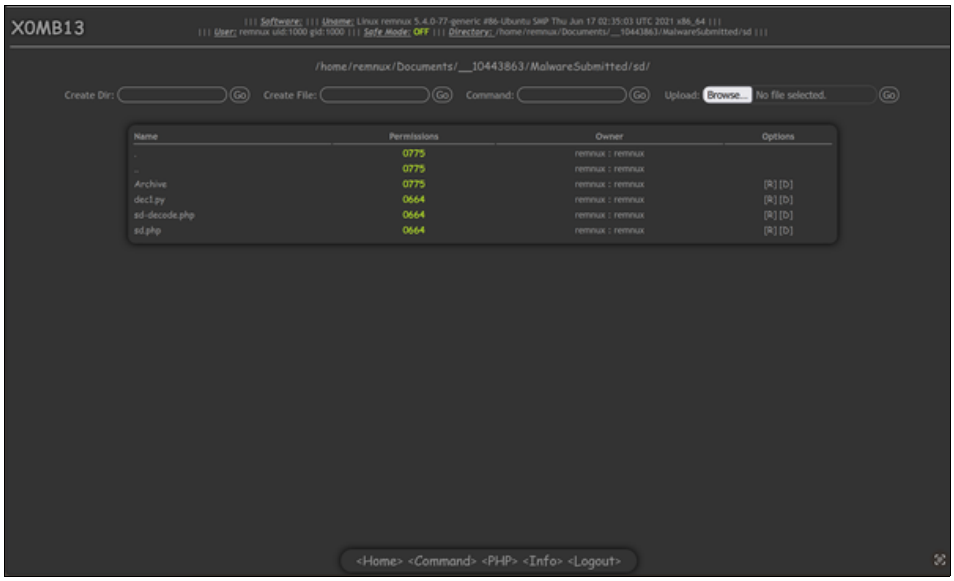

Figure 2. - sd.php webshell interface. Threat Actor (TA) would have access to this interface remotely to conduct various actions like upload additional files, create directories and files, run commands and more.

6ce087b904af8a01aae73ac77d81822ad41799f89a5d301dce45191c897012aa

Tags

backdoor trojan webshell

Details

Name	osker.aspx
Size	107843 bytes
Type	data
MD5	fcb8a6a264d05f1689c9dce5824b217d
SHA1	001e4906879e78d567a30502638233f34292504a
SHA256	6ce087b904af8a01aae73ac77d81822ad41799f89a5d301dce45191c897012aa
SHA512	703437c5742f343cabc6023698e031f0c4167252e9679d4e4fd13d9703f27de21faa7edf275bd9a39c4b2e454a83c43d555849ae61a0897ac1da9ed6be820d4d
ssdeep	3072:K+mYWYJo8+p87xbsTttEtizQhch+mYWYJo8+pO:K+mYDnhch+mYDD
Entropy	6.343192

Antivirus

IKARUS	Trojan.ASP.Agent
McAfee	ASP/Backdoor.i
Varist	JS/Agent.AIW

YARA Rules

```
rule CISA_10443863_02 : backdoor remote_access_trojan webshell exploitation information_gathering remote_access accesses_remote_machines anti_debugging captures_system_state_data controls_local_machine compromises_data_availability compromises_data_integrity fingerprints_host installs_other_components
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10443863"
    Date = "2023-05-11"
    Last_Modified = "20230522_1200"
    Actor = "n/a"
    Family = "n/a"
    Capabilities = "accesses-remote-machines anti-debugging captures-system-state-data controls-local-machine compromises-data-availability compromises-data-integrity fingerprints-host installs-other-components"
    Malware_Type = "backdoor remote-access-trojan webshell"
    Tool_Type = "exploitation information-gathering remote-access"
    Description = "Detects interactive ASP NET webshell samples"
    SHA256 = "ea98368f6ecb5281654a6a9e4c649ef9b53860f1ee32340145b61e0e42e1072a"
  strings:
    $s0 = { 3c 25 40 20 50 61 67 65 20 4c 61 6e 67 75 61 67 65 3d 22 43 23 22 }
    $s1 = { 62 61 73 65 36 34 ( 44 | 64 ) 65 63 6f 64 65 }
    $s2 = { 53 65 6c 65 63 74 20 2a 20 66 72 6f 6d 20 57 69 6e 33 32 5f 50 72 6f 63 65 73 73 }
    $s3 = { 53 45 4c 45 43 54 20 2a 20 46 52 4f 4d }
    $s4 = { 73 71 6c 63 6d 64 2e 65 78 65 }
    $s5 = { 63 6d 64 2e 65 78 65 }
    $s6 = { 49 49 53 20 56 65 72 73 69 6f 6e }
    $s7 = { 43 72 65 61 74 65 4e 6f 57 69 6e 64 6f 77 }
  condition:
    all of them
}
```

ssdeep Matches

No matches found.

Relationships

6ce087b904...	Related_To	b63c95300c8e36b5e6d3393da12931683796f88fd4601ba8364658b4d12ac05b

Description

This sample is an ASP .NET webshell. The webshell code was padded with junk code for detection evasion. The beginning of the webshell code can be seen in Figure 3. It is possible to access the webshell interactively via browser to view the GUI as seen in Figure 4.

This webshell has the ability to enumerate drive name and type, software, operating system versions, processes, and users, and has ability to copy, create and delete files, directories and databases. Furthermore, this webshell is able to upload, download, run and execute commands using cmd.exe and sqlcmd.exe. This webshell has the ability to interact with and manipulate SQL databases. Furthermore, this webshell uses Windows Management Instrumentation (WMI) Management Objects to query processes, users and network domains. It is also able to encode and decode data using base64.

---Notable Strings Begin---
osker
321
<%@ Page Language="C#"
base64Decode
Select * from Win32_Process
Select * from Win32_Process Where ProcessID
Add_Table_Row(tbl, "Server IP", Request.ServerVariables["LOCAL_ADDR"]);
Add_Table_Row(tbl, "Host Name", Dns.GetHostName());//Environment.MachineName);
Add_Table_Row(tbl, "IIS Version", Request.ServerVariables["SERVER_SOFTWARE"]);
Add_Table_Row(tbl, "IIS APPPOOL Identity", Environment.UserName);
Add_Table_Row(tbl, "OS Version", Environment.OSVersion.ToString());
myconn = new SqlConnection(connections.Text);
myconn.Open();
string command = query;
mycomm = new SqlCommand(command, myconn);
SqlDataReader dr = mycomm.ExecuteReader();
string query = "Select * from Win32_Process Where ProcessID = \"" + processName + "\"";
ManagementObjectSearcher searcher = new ManagementObjectSearcher(query);
ManagementObjectCollection processList = searcher.Get();
ManagementObjectSearcher QS=new ManagementObjectSearcher(new SelectQuery(query));
---Notable Strings End---

Screenshots

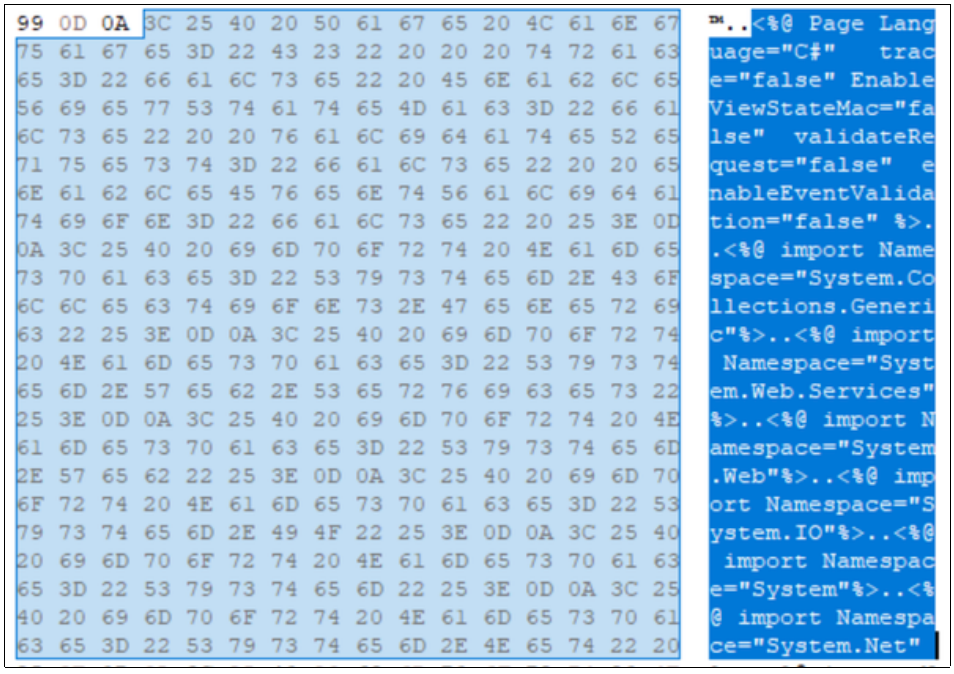

Figure 3. - Beginning of osker.aspx webshell code.

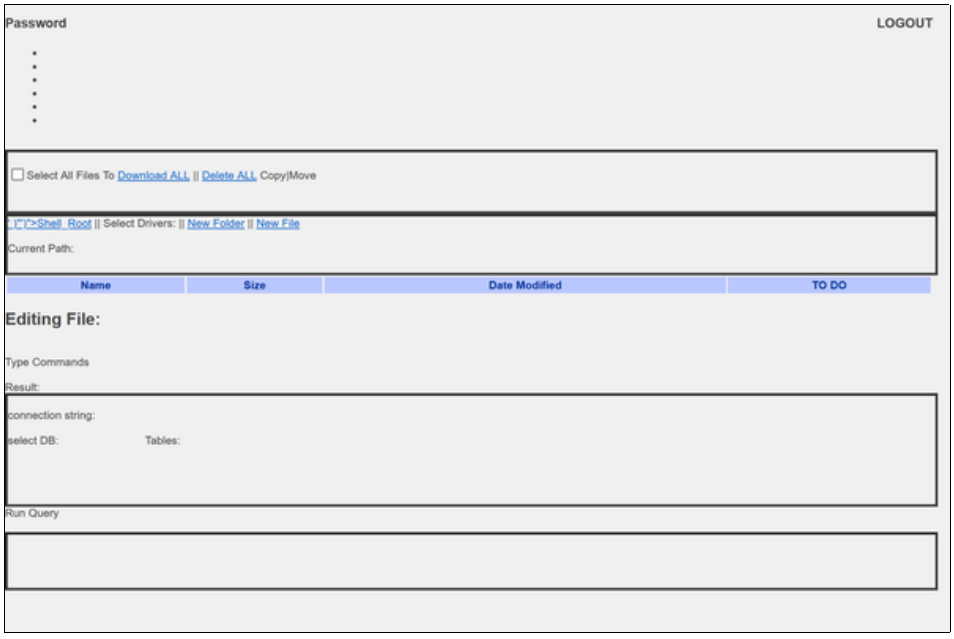

Figure 4. - Web interface for osker.aspx webshell. The webshell interface password is “321”.

b63c95300c8e36b5e6d3393da12931683796f88fd4601ba8364658b4d12ac05b

Tags

backdoor trojan webshell

Details

Name	App_Web_jl37rjxu.dll
Size	163840 bytes
Type	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
MD5	71323c956317b6b2c8e4ed4595ccfe5a
SHA1	7ebd98f97f61cabff05438dfac34d0331ce233aa
SHA256	b63c95300c8e36b5e6d3393da12931683796f88fd4601ba8364658b4d12ac05b
SHA512	2da3716aab9c9a8a85705c1372c4d75250dc021caa4f3b7566f6c142bdb3a45a063ec5f343b15b9be6056890768e80e7512f6ddbb86de178c475a160f56c0dad
ssdeep	3072:XEFKnpDtdIftAIe66rOqhTG0t7x2IftAIe66rOqhTG0:XEyJXmtQTO+ymtQTO+
Entropy	5.776030

Antivirus

Antiy	Trojan[Backdoor]/ASP.WebShell
Avira	BDS/Redcap.euknj
Bitdefender	Trojan.Generic.33706396
Emsisoft	Trojan.Generic.33706396 (B)
McAfee	RDN/Generic BackDoor
Zillya!	Backdoor.WebShell.Script.653

YARA Rules

- rule CISA_10443863_03 : backdoor remote_access_trojan webshell exploitation information_gathering remote_access accesses_remote_machines anti_debugging captures_system_state_data controls_local_machine compromises_data_availability compromises_data_integrity fingerprints_host installs_other_components
  {

```
    meta:
        Author = "CISA Code & Media Analysis"
        Incident = "10443863"
        Date = "2023-05-16"
        Last_Modified = "20230605_1500"
        Actor = "n/a"
        Family = "n/a"
        Capabilities = "accesses-remote-machines anti-debugging captures-system-state-data controls-local-machine compromises-
data-availability compromises-data-integrity fingerprints-host installs-other-components"
        Malware_Type = "backdoor remote-access-trojan webshell"
        Tool_Type = "exploitation information-gathering remote-access"
        Description = "Detects .NET DLL webshell samples"
        SHA256 = "b63c95300c8e36b5e6d3393da12931683796f88fd4601ba8364658b4d12ac05b"
    strings:
        $s0 = { 53 00 65 00 6c 00 65 00 63 00 74 00 20 00 2a 00 20 00 66 00 72 00 6f 00 6d 00 20 00 57 00 69 00 6e 00 33 00 32
00 5f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 }
        $s1 = { 62 61 73 65 36 34 ( 44 | 64 ) 65 63 6f 64 65 }
        $s2 = { 53 00 45 00 4c 00 45 00 43 00 54 00 20 00 2a 00 20 00 46 00 52 00 4f 00 4d }
        $s3 = { 49 00 49 00 53 00 20 00 41 00 50 00 50 00 50 00 4f 00 4f 00 4c }
        $s4 = { 4d 61 6e 61 67 65 6d 65 6e 74 4f 62 6a 65 63 74 }
        $s5 = { 43 72 65 61 74 65 4e 6f 57 69 6e 64 6f 77 }
        $s6 = { 73 71 6c 71 75 65 72 79 }
    condition:
        all of them
}
```

ssdeep Matches

No matches found.

Relationships

b63c95300c...	Related_To	6ce087b904af8a01aae73ac77d81822ad4179 9f89a5d301dce45191c897012aa

Description

This is a 32-bit .NET Dynamic-Link Library (DLL) file. This sample is a ASP .NET webshell and is related to the osker.aspx file. These webshells may affect Microsoft Exchange Servers and IIS services exploited by the ProxyLogon vulnerability. This sample is a .NET DLL file that is created by the ASP.NET Runtime when ASPX script is seen for the first time on the system. The capabilities and functions are identical to the osker.aspx file.

Relationship Summary

6ce087b904...	Related_To	b63c95300c8e36b5e6d3393da12931683796f 88fd4601ba8364658b4d12ac05b
b63c95300c...	Related_To	6ce087b904af8a01aae73ac77d81822ad4179 9f89a5d301dce45191c897012aa

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.