Threat Research

Know Your Enemy: Tracking A Rapidly Evolving APT Actor

October 31, 2013 | by Ned Moran, Thoufique Haq

Between Oct. 24–25 FireEye detected two spear-phishing attacks attributed to a threat actor we have previously dubbed admin@338.[1] The newly discovered attacks targeted a number of organizations and were apparently focused on gathering data related to international trade, finance, and economic policy. These two attacks utilized different malware families and demonstrate an ability to quickly adapt techniques, tactics, and procedures (TTPs).

Investor Guide and Contact List Lure

On Friday Oct. 25, 2013, FireEye detected an attempted targeted campaign against the following:

- The Central Bank of a Western European government
- An International organization involved in trade, economic, and financial policy
- A U.S.-based think tank
- A high-ranking government official for a country in the Far East

This spear-phish email, shown in Figure 1, contained a malicious Word document attachment that exploited the CVE-2012-0158 vulnerability.

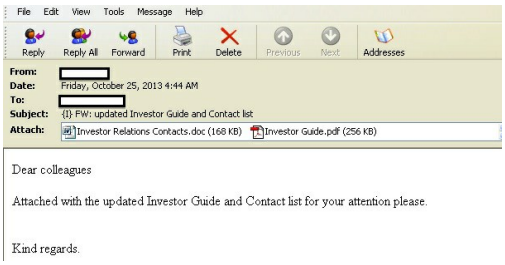

Figure 1: Spear-phish email used in a recent admin@338 attack

The malicious Word document had the following properties:

- File: Investor Relations Contacts.doc
- MD5: 875767086897e90fb47a021b45e161b2

Upon opening the file, a malicious executable with the MD5 hash value of c5d8b7c8e2f50b171840e071f8a079b6 is then written to C:\Windows\wmiserver.exe and subsequently executed. This executable is a variant of the Bozok RAT, which was configured to connect to its command-and-control (CnC) server at microsoft.mrbasic.com and www.microsoft.mrbasic.com with the Bozok connection password of "wwwst@Admin". We observed the domain microsoft.mrbasic.com resolving to 58.64.153.157 on Oct. 26, 2013.

Bozok RAT Capabilities and Behavior

Bozok, like many other popular RATs, is freely available [2]. The author of the Bozok RAT goes by the moniker "Slayer616" and has created another RAT known as Schwarze Sonne, or "SS-RAT" for short. Both of these RATs are free and easy to find — various APT actors have used both in previous targeted attacks.

Unlike SS-RAT, Bozok is still actively maintained, with two new updates released in October that fixed some bugs and added language support for Spanish, Arabic, Bulgarian, Polish, and French. These and other improvements have made Bozok intuitive and easy to use. As shown in Figure 2, it features an easy-to-navigate graphical user interface that enables operators to point and click their way through the entrenchment, lateral movement, and exfiltration process.

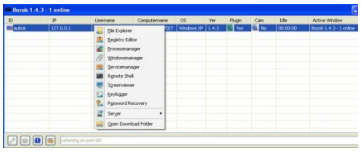

Figure 2: The Bozok interface

Once an endpoint is infected with Bozok, the attacker can do the following:

- Upload and download files to and from the target's machine
- Launch and kill processes
- Modify the registry
- Grab stored passwords

Attackers can also use the Bozok graphical user interface to run arbitrary shell commands on the target machines, as shown in Figure 3.

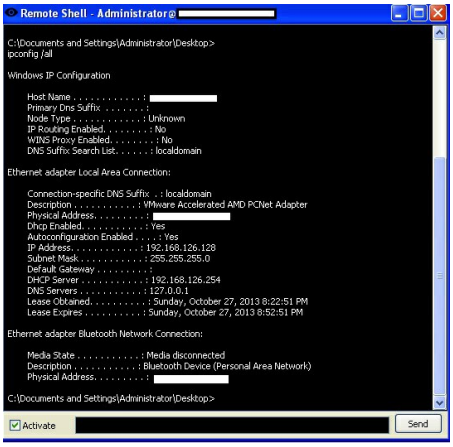

Figure 3: Running shell commands with Bozok.

A DLL plugin — which can be downloaded and loaded through the Bozok GUI control panel onto the infected endpoint — extends the RAT's functionality with the following commands:

- `StartVNC`
- `StopVNC`
- `StartWebcam`
- `StopWebcam`
- `SendCamList`
- `IsWebcam`
- `DeleteKeylog`

- GetKeylog
- StopKeylog
- QueryScreen

Bozok stores its configuration parameters in the resource section of the executable file. The parameters are contained in a PE manifest called "CFG". The configuration for the Bozok variant from the current attack (wmiserver.exe c5d8b7c8e2f50b171840e071f8a079b6) is shown in Figure 4.

Figure 4: Bozok PE manifest

The following parameters are stored in this manifest:

```
ID = aubok

Mutex = 80lJsYqFulHpg

Filename = wmiserver.exe

Startup Entry Name = wmiupdate

Plugin filename = ext.dat

Connection password = wwwst@Admin

Connection port = 80

Connection servers = www.microsoft.mrbasic.com, microsoft.mrbasic.com
```

These parameters are configured at the build time of the RAT. The mutex is randomly generated at the build time of the RAT and is used to ensure that only one copy of the malware is running on a targeted machine.

Upon initial infection, Bozok emits the outgoing initial network beacon traffic shown in Figure 5.

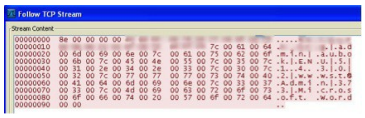

Figure 5: Bozok beacon traffic

The beacon contains the length of the packet in little-endian format between the offsets 04. The following data follows this in a wide-string format with a pipe separator as follows:

LengthofData | Hostname | Username| ID | LocaleInfo | OS Version | RAT Version | 0 | 2 | ConnectionPassword | IdleTime | ActiveWindowName

The beacon also contains a hardcoded connection password "wwwst@Admin" in the beacon, which is used to authenticate when connecting to its GUI control panel.

Attribution

We have attributed this attack to the admin@338 actor that we described in our report *Poison Ivy: Assessing Damage and Extracting Intelligence* [3]. The admin@338 actor has also used the same "wwwst@Admin" string as a password in previously observed Poison Ivy samples used in targeted attacks. For example, the file SnowdenBook.doc (MD5: d40f50d37d51f6cd92e98c4da4e066ff) dropped a Poison Ivy sample that used "wwwst@Admin" as a password.

Additionally, the CnC IP of 58.64.153.157, used by the Bozok variant (MD5: c5d8b7c8e2f50b171840e071f8a079b6) dropped by the Investor Relations Contacts.doc lure has also hosted a number of other CnC domains linked to the admin@338 actor. On Oct. 27, 2013 we observed the following known admin@338 domains resolving to 58.64.153.157:

consilium.dnset.com

consilium.dynssl.com

consilium.proxydns.com

dnscache.lookin.at

ecnet.rr.nu

european.athersite.com

hq.dsmtp.com

hq.dynssl.com

ipsecupdate.byinter.net

itagov.byinter.net

microsoft.acmetoy.com

microsoft.dhcp.biz

microsoft.dynssl.com

microsoft.ftpserver.biz

microsoft.instanthq.com

microsoft.isasecret.com

microsoft.lookin.at

microsoft.proxydns.com

microsoft.wikaba.com

microsofta.byinter.net

microsoftb.byinter.net

phpdns.myredirect.us

sslupdate.byinter.net

svchost.lookin.at

svchost.passas.us

teamware.rr.nu

webserver.dynssl.com

webserver.fartit.com

webserver.freetcp.com

www.consilium.dnset.com

www.consilium.dynssl.com

www.consilium.proxydns.com

www.hq.dsmtp.com

www.hq.dynssl.com

www.microsoft.acmetoy.com

www.microsoft.dhcp.biz

www.microsoft.dsmtp.com

www.microsoft.dynssl.com

www.microsoft.instanthq.com

www.microsoft.isasecret.com

www.microsoft.proxydns.com

www.microsoft.wikaba.com

www.svchost.ddns.info

www.svchost.dyndns.pro

www.svchost.dynssl.com

www.verizon.dynssl.com

www.verizon.itemdb.com

www.verizon.proxydns.com

www.webserver.dynssl.com

www.webserver.fartit.com

www.webserver.freetcp.com

We previously detected the same admin@338 actor using the Bozok RAT on Jan. 6, 2013. In this attack, the admin@338 actor emailed the malicious spreadsheet EcoMissionList.xls (MD5: f10e89c194742a9ad98efbf1650084f3) to the same international organization involved in trade, economic, and financial policy targeted by the more recent Investor Relations Contacts.doc lure (MD5: 875767086897e90fb47a021b45e161b2). The malicious EcoMissionList.xls spreadsheet dropped a Bozok variant with an MD5 of a45d3564d1fa27161b33712f035a5962. This Bozok implant connected to CnC servers at www.microsoftupdate.dynssl.com with the password of "gwxpass". A previous admin@338 Poison Ivy sample (MD5: d22e974b348be44dde5566267250ff0e) was configured with the similar password "gwx@338".

Investor Relations Contacts-AsiaPacific Lure

During our investigation of the most recent Bozok sample within Investor Relations Contacts.doc, we discovered a related attack that occurred on Oct. 24, 2013 — one day before the wave of Bozok-fueled spear phishes. This attack also utilized spear phishing as a delivery mechanism by sending the following malicious document to the same U.S.-based think tank targeted by admin@338 with the Bozok RAT on Oct. 25:

- File: Investor Relations Contacts-AsiaPacific.doc
- MD5: c6de1ca261662aca6b8a782075a8671f

The malicious document dropped an implant with the MD5 f7fb380f2b0c22c12f605ce9b4b162f2 to C:\Documents and Settings\admin\Application Data\svchost.exe. We detect this implant as Backdoor.APT.FakeWinHTTPHelper. This sample connected to CnC servers at www.dpmc.dynssl.com and www.dataupdate.dynssl.com.

The domain www.dpmc.dynssl.com resolved to Oct. 24, 2013, and www.dataupdate.dynssl.com resolved to 58.64.153.157 on Oct. 21, 2013.

Though the Oct. 24 attack did not use the Bozok RAT, it is likely that the admin@338 actor was also responsible for this attempted intrusion for the following reasons:

- We have previously observed the admin@338 actor use Backdoor.APT.FakeWinHTTPHelper in targeted attacks.
- The same 58.64.153.157 IP address was used in both attacks.
- The same US-based think-tank was targeted in both attacks.

Conclusions

These consecutive incidents, Backdoor.APT.FakeWinHTTPHelper on Oct. 24 and Bozok RAT on Oct. 25, demonstrate that the admin@338 actor has the ability to rapidly alter TTPs. Further, the admin@338 actor can integrate publicly available RATs such as Poison Ivy and Bozok as well as custom RATs such as Backdoor.APT.FakeWinHTTPHelper into their arsenal. Organizations must be prepared to defend themselves from this wide array of attacks.

Footnotes:

[1] For more on admin@338, see our previous blog entry on Poision Ivy

[2] http://ss-rat.blogspot.com/

[3] This report is available at here.

PREVIOUS POST

NEXT POST

Contact Us
+1 877-347-3393

Stay Connected

Site Language
English