New Targeted Attack Group Buys BIFROSE Code, Works in Teams

- Posted on:December 10, 2015 at 3:55 am
- Posted in:Targeted Attacks
- Author: Trend Micro

By Razor Huang (Threats Analyst)

Recently, we uncovered a new cyber-espionage attack by a well-funded and organized group targeting companies close to governments and in key industries mostly in Asia. These targets include privatized government agencies and government contractors, as well as companies in the consumer electronics, computer, healthcare, and financial industries.

This group has been active since 2010. We dub this operation Shrouded Crossbow, after a mutex in a backdoor the group developed. Our research indicates that the group has sufficient financial resources to purchase the source code of a widely available malware tool, and the human resources to design improved versions of its own backdoors based on this.

BIFROSE, KIVARS and XBOW

BIFROSE, also known as Bifrost, was sold underground for up to $10,000 in the past. We have seen it used in a targeted attack on government offices and the "Here You Have Mail" spam campaign. Despite BIFROSE's well-known network traffic and behaviors, however, the group was still able to make full use of it in its operation.

The following code snippet shows BIFROSE sending its phone home message, which contains the victim's profile information, to its command-and-control (C&C) server.


11112
127.0.0.1|default_zz|HOSTNAME|Administrator|10.0.3||1|-1|0|1868|1|1|0|0|982bc1d
a|C:\Documents and Settings\Administrator\Recent|C:\Documents and Settings\Admi
nistrator\Desktop|C:\Documents and Settings\Administrator\My Documents|US|00000
409|

Figure 1. The phone home message of BIFROSE

Another backdoor used by the operation since 2010 is KIVARS. While it is similar to PLUGX because of its two components (a loader and the main backdoor), KIVARS has a much stronger connection with BIFROSE because of its phone home message format.

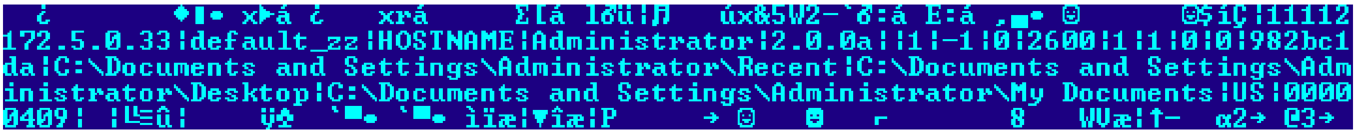
11112
172.5.0.33|default_zz|HOSTNAME|Administrator|2.0.0a||1|-1|0|2600|1|1|0|0|982bc1
da|C:\Documents and Settings\Administrator\Recent|C:\Documents and Settings\Adm
inistrator\Desktop|C:\Documents and Settings\Administrator\My Documents|US|0000
0409|

Figure 2. The phone home message of KIVARS

Although KIVARS is not as heavy in terms of functions when compared with BIFROSE, it is still a pretty handy backdoor for the group. In fact, in 2013, KIVARS started offering an upgraded 64-bit version, in line with the rise of 64-bit systems.

What we think happened is that the group purchased the source code of BIFROSE, and after improving its functions, the group then designed a new installation flow, developed a new builder to create unique loader-backdoor pairs, and made more simple and concise backdoor capabilities, resulting in a new backdoor—KIVARS. This could mean that the operation is either backed financially by its sponsors or the group has the funds and resources to improve on an existing backdoor.

Interestingly, some KIVARS backdoors' PDB (program database) paths betray the code name of KIVARS to be "BR" + "{year}". We think that BR mostly likely stands for Bifrose RAT.

PDB PATHS
Q:\Projects\Br2012\Release\ttt.pdb
Q:\Projects\Br2012\Release\insbr.pdb
Q:\Projects\Br2012\Release\svc.pdb
P:\Projects\Br2014\Release\br2014.pdb

Figure 3. Some of KIVARS' PDB Paths

The operation also made use of another in-house developed backdoor, XBOW. The development of XBOW can be traced back to the middle of 2010 and is inspired by the design of BIFROSE and KIVARS.

This assembly screenshot of XBOW shows the "Recent," "Desktop," and "Program" folder paths, which are also present in the BIFROSE and KIVARS phone home messages.

Figure 4. Snippet of XBOW assembly code

Later in the middle of 2011, some XBOW variants provided a "Find Passwords" option, which is a functionality also available in BIFROSE. This lends further proof to our BIFROSE purchase theory.

Clear Operational Roles

One other interesting finding we discovered about XBOW, which led to the naming of Operation Shrouded Crossbow, is a mutex created by the said backdoor. The name of this mutex starts with "zhugeliannu."

The format of the mutex name is as follows:

- *zhugeliannu{1 byte possible project version}{builder identity}{compile date}*

The mutex name format served as a guideline for the threat actors building XBOW.

Compile Date	Mutex Name
2011/3/28 01:41	zhugeliannu2zhang3
2011/11/8 01:18	zhugeliannu2xue1108
2012/6/11 00:11	zhugeliannu2lxy0611
2012/10/16 01:00	zhugeliannu1016liang
2013/2/27 02:25	zhugeliannu2cao0227
2014/3/30 08:31	zhugeliannu2cao0330

Examining the {builder identity} sections of the mutex names, we conclude that there are at least 10 threat actors who were responsible for building XBOW and for sending it to victims. This small team may have served as the tool developer team of the attack group.

In addition to the above team, we believe that another team, in charge of infiltration, is responsible for performing a successful point of entry in the network using spear-phishing attacks with malicious attachments. The attached files are either a .RAR archive file that uses the RTLO (right to left override) technique, or a .EXE file with fake documents presenting themselves as either breaking news, resumes, shared information, government data, or meeting requests. They configure the tools' builder, specifying the infection method, assigned C&C, file name when installed, etc.

Maintaining the group's C&C servers could be assigned to a third team. There are more than 100 C&Cs used in the operation, some registered via free dynamic DNS or by the threat actors while some are IPs. The C&Cs are organized depending on their use. We observed that C&C maintenance activities such as IP changes or renewal of expired domains happen in an organized fashion. They are still registering new domains to this day.

Implications on Enterprises

Enterprises faced with targeted attacks like these have no chance against well-funded, organized groups unless they apply the same attention and focus on their own network to detect intrusions and anomalies and respond appropriately. Network defense platforms like Deep Discovery enables IT admins to detect, analyze and respond to these kinds of threats.

I have presented my findings last week in AVAR 2015, along with my other colleagues from Trend Micro who have discussed the code improvements in DYRE, a notorious banking Trojan that can rival ZeuS, and the active development of URSNIF.

Related Posts:

- Hacktivist Group CyberBerkut Behind Attacks on German Official Websites
- MERS News Used in Targeted Attack against Japanese Media Company
- New Router Attack Displays Fake Warning Messages
- Over a Decade and Still Running: Targeted Attack Tool Hides Windows Tasks

Featured Stories

- 2016 Predictions: The Fine Line Between Business and Personal
- Pawn Storm Targets MH17 Investigation Team
- FBI, Security Vendors Partner for DRIDEX Takedown
- Japanese Cybercriminals New Addition To Underground Arena
- Follow the Data: Dissecting Data Breaches and Debunking the Myths

Recent Posts

- New Targeted Attack Group Buys BIFROSE Code, Works in Teams
- Adobe Flash Player Fixes 79 Bugs; Microsoft Issues 12 Patches in December Patch Tuesday
- Blog of News Site "The Independent" Hacked, Leads to TeslaCrypt Ransomware
- The German Underground: Buying and Selling Goods via Droppers
- Out in the Open: Accessibility in the North American Underground

2016 Security Predictions

- From new extortion schemes and IoT threats to improved cybercrime legislation, Trend Micro predicts how the security landscape is going to look like in 2016. Read more

Popular Posts

High-Profile Mobile Apps At Risk Due to Three-Year-Old Vulnerability
Trend Micro, NCA Partnership Leads to Arrests and Shutdown of Refud.me and Cryptex Reborn
Siri's Flaw: Apple's Personal Assistant Leaks Personal Data
Blog of News Site "The Independent" Hacked, Leads to TeslaCrypt Ransomware
Cybercriminals Improve Android Malware Stealth Routines with OBAD

Latest Tweets

- @Scardanelli1748 You can check the paper here bit.ly/1QcLFMs
  about 44 mins ago
- The Independent hack sees new infection chain with #CryptoLocker #ransomware bit.ly/1HU0kcZ
  about 12 hours ago
- Learn more about the "dropper scheme" that the German underground is now known for: blog.trendmicro.com/trendlabs-secu…

about 15 hours ago

Stay Updated

Email Subscription

Your email here

Subscribe