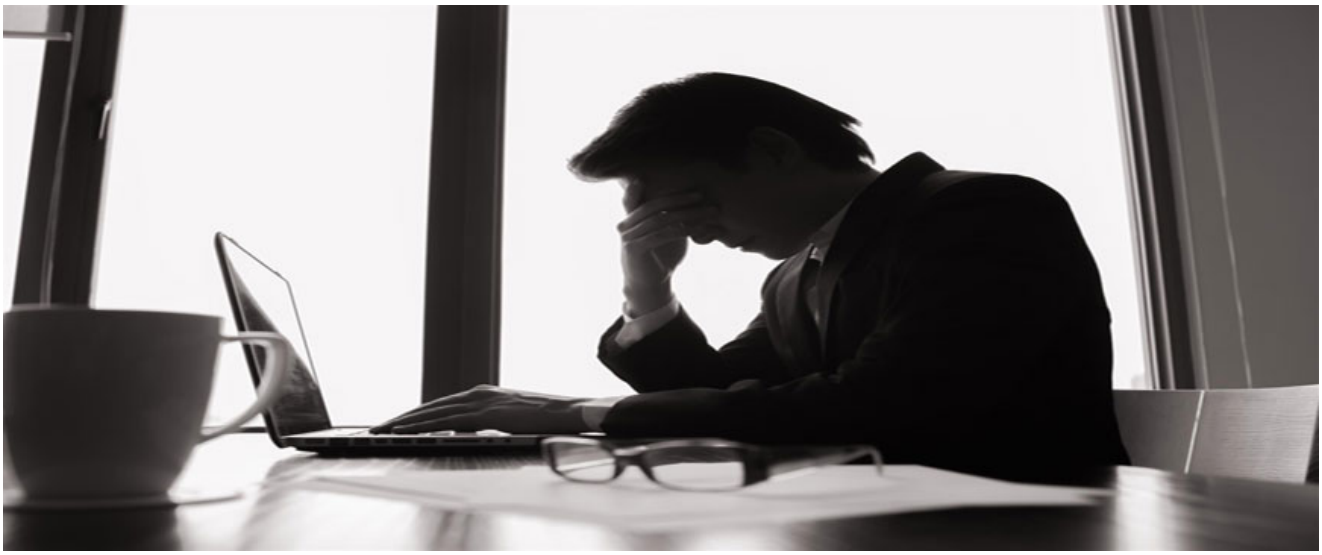
Shrouded Crossbow Creators Behind BIFROSE for UNIX

trendmicro.com/en_us/research/16/c/threat-actors-behind-shrouded-crossbow-creates-bifrose-for-unix.html

March 1, 2016



We recently came across a variant of the BIFROSE malware that has been rewritten for UNIX and UNIX-like systems. This is the latest tool developed by attackers behind operation Shrouded Crossbow, which have produced other BIFROSE variants such as KIVARS and KIVARS x64. UNIX-based operating systems are widely used in servers, workstations, and even mobile devices. With a lot of highly confidential data found in these servers and devices, a UNIX version of BIFROSE can certainly be classified as a threat.

Capable Hands

BIFROSE has been updated by Shrouded Crossbow specifically for the campaigns they pursue. Some of their victims have already been compromised by both Windows and UNIX versions of BIFROSE. Historically, Shrouded Crossbow has used BIFROSE to target privatized government agencies, government offices, and government contractors, as well as companies in the consumer electronics, computer, healthcare, and financial industries.

BIFROSE Evolution Under Shrouded Crossbow	
2004	BIFROSE was developed by ksv as a trojan known to have infected Windows 95 through Windows 7.

2010	Shrouded Crossbow developed KIVARS 2010 – Dropped by malware detected as TROJ_FAKEWORD.A (SHA1 218be0da023e7798d323e19e950174f53860da15) and only affects 32-bit systems Only encrypts the “MZ” magic byte for the backdoor payload
2013	Shrouded Crossbow developed KIVARS x64 Can work in 32-bit and 64-bit environments Payload is now encrypted using the modified RC4
2014	Shrouded Crossbow developed UNIX BIFROSE

UNIX BIFROSE

UNIX BIFROSE was created after the Shrouded Crossbow rewrote BIFROSE and compiled it into an Executable and Link Format (ELF) which is a standard executable file for UNIX and UNIX-like systems. Its code is completely changed compared to the Windows version, but still having almost the same protocol and command-and-control (C&C) commands. Both Windows and UNIX versions can communicate with the original Bifrost C&C server. One big difference between the Windows and UNIX version is that UNIX BIFROSE has less backdoor functions compared to the original BIFROSE.

PHONE HOME PACKETS FOR UNIX AND WINDOWS

UNIX

> <victim IP>|unix|<hostname>|<username>|5.0.0.0|0|1|1|0|575|0|0|0|0|None|||||

Windows

> <victim IP>|default_zz|<hostname>|
> <username>|2.0.0a||1|-1|0|2600|1|1|0|0|982bc1da|C:\Documents and Settings\Administrator\Recent|C:\Documents and Settings\Administrator\Desktop|C:\Documents and Settings\Administrator\My Documents|US|00000409|

In the phone home packet, BIFROSE will register with a default assigned name on C&C. The default name for the Windows version of BIFROSE is *default_zz*, whereas for UNIX, the default name is *unix*. The attacker can easily change these names at a later time. The initial malware installed will be 2.0.0a for Windows, and 5.0.0.0. for UNIX. The Windows version, once connected to the c&c server, will contain the disk serial number, locale, and keyboard layout that identifies the victims and helps the attackers manage the tools needed for the attack. The However, the previously mentioned information will not be available for the UNIX version.

UNIX BIFROSE also provides a “create remote shell” which is perfect for skilled attackers who are familiar with the UNIX system.

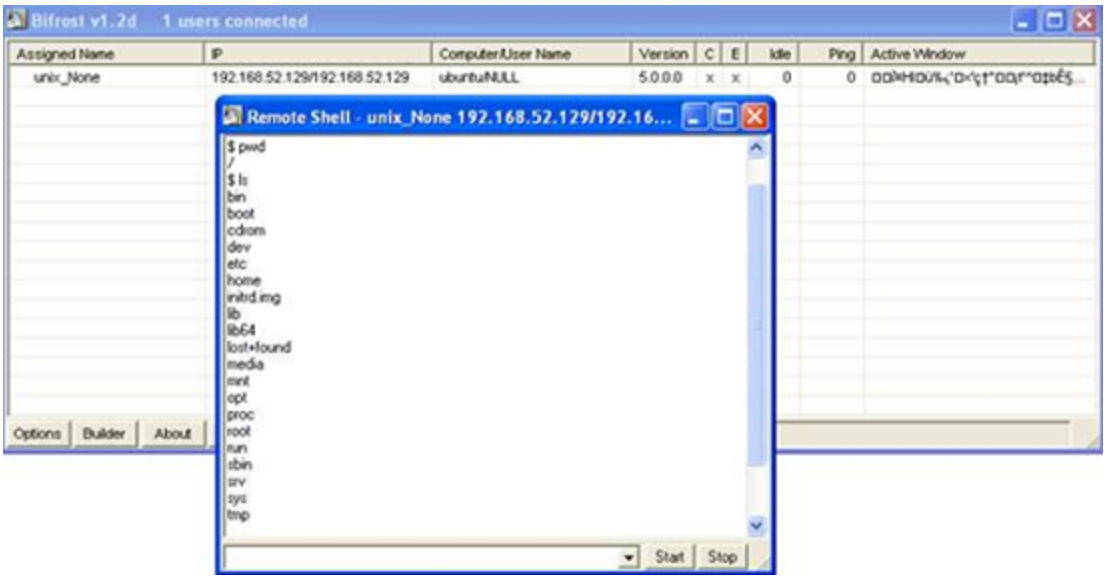


Figure 1. "create remote shell" command for UNIX BIFROSE

Malware Crossing Platforms

After testing the UNIX BIFROSE version, we figured out that it has no problem communicating with the BIFROSE server console used by the original BIFROSE (the Windows version). Our research indicates that a network can be infected by both Windows and UNIX versions of the malware. This ensures that regardless of OS used by the victim, the threat actor is ready and able to capture and communicate with any server.

With BIFROSE used as a component for recent targeted attacks, we studied the new variant to see its strength in a sustained attack. UNIX BIFROSE can be used in the lateral movement phase of a targeted attack. It can be deployed to control a Linux server in the victim's network. It can also find other vulnerable Linux units which it can infect to sustain the attack further.

While half of the threat of UNIX BIFROSE falls on its capabilities, the other half falls on Shrouded Crossbow's capability to create tools such as updated versions of BIFROSE.

As far as which platform BIFROSE will move to next, it will not be a matter of time. Instead, it will be a matter of need. If Shrouded Crossbow needs BIFROSE for iOS or Android, it is possible, even if they have to rewrite the code. And looking at how they were able to create UNIX BIFROSE, an OS X version may not be far off.

Implications on Enterprises

Upon the first signs of abnormal activities, such as those seen through network and mail logs, IT admins must be prepared and quick to respond. As we've mentioned in our past post, 7 Places to Check for Signs of a Targeted Attack in Your Network, network activities such as logins and emails during "abnormal" times need to be checked.

When enterprises face targeted attacks, they have to apply the same attention and focus on their own network to detect intrusions and anomalies and respond appropriately. Network defense platforms like Trend Micro Deep Discovery, Deep Security, and ServerProtect enable IT admins to detect, analyze and respond to these kinds of threats. They can detect BIFROSE behaviors such as malicious behavior, command-and-control communications, lateral movement, and data exfiltration.

Here are the hashes for ELF_BIFROSE.ZTDA and their C&C servers:

SHA1	C&C
3d3bb509f307db97630c297bdb985c83d8a40951	103.246.247.103 202.133.245.251
5d8b228e3014b4eb579e380b3a1113dd8c0d999a	58.64.185.12

Malware

We came across a variant of the BIFROSE malware rewritten for UNIX and UNIX-like systems. This is the latest tool from the attackers behind operation Shrouded Crossbow, which have produced other BIFROSE variants such as KIVARS and KIVARS x64.

By: Razor Huang March 01, 2016 Read time: (words)

Content added to Folio