Hidden Cobra

Author: James Barnett

Executive Summary

On 9 September the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the Department of Defense (DoD) jointly published updates to their Malware Analysis Reports (MARs) about trojan malware variants known as BADCALL[1] and ELECTRICFISH[2]. The reporting agencies attributed these malware variants to the North Korean government, whose malicious cyber activities are commonly referred to as HIDDEN COBRA.

The MAR for BADCALL describes the malware as a set of 32-bit Windows executable files that force compromised systems to function as proxy servers, plus another piece of malware for the Android operating system that functions as a remote access tool (RAT). The updated MAR for ELECTRICFISH includes a more detailed explanation of the malware's command line arguments as well as an analysis of a new variant of the malware that uses more advanced Transmission Control Protocol (TCP) session headers to establish its initial connection.

The intended targets of BADCALL and ELECTRICFISH are unknown, but HIDDEN COBRA activity has historically been focused against the media, aerospace, and financial industries, as well as other critical infrastructure industries.[3] The following advisories from the Infoblox Cyber Intelligence Unit provide additional information and context about past HIDDEN COBRA activity:

- HIDDEN COBRA: ELECTRICFISH (May 2019)[4]
- HIDDEN COBRA: HOPLIGHT (Apr 2019)[5]
- HIDDEN COBRA: FASTCash (Oct 2018)[6]
- HIDDEN COBRA: Keymarble (Aug 2018)[7]
- HIDDEN COBRA: Typeframe (June 2018)[8]
- HIDDEN COBRA: Brambul Worm & Joanap RAT (May 2018)[9]
- HIDDEN COBRA: Fallchill RAT & Volgmer Trojan (Nov 2017)[10]

Analysis

The Infoblox Cyber Intelligence Unit outlined the technical details of ELECTRICFISH in our May 2019 report, referenced above. The technical details of that report are still consistent with the updated MAR that U.S. government agencies published today. As such, this Cyber Threat Advisory will focus primarily on BADCALL.

ELECTRICFISH

The updated MAR for ELECTRICFISH includes a SHA256 checksum for a new variant that uses more complex TCP session headers when establishing connections. It also contains more extensive descriptions of ELECTRICFISH's command line arguments than the descriptions included in the initial MAR.

BADCALL

According to the joint report, BADCALL includes three different 32-bit Windows executables designed to hijack a system's networking features so that threat actors can use the compromised system as a proxy server. When executed, each of BADCALL's Windows variants first attempts to disable the Windows Firewall by modifying the following registry key:

```
SYSTEM\CurrentControlSet\Services\SharedAccess\
Parameters\FirewallPolicy\StandardProfile\
GloballyOpenPorts\\List
```

After disabling the Windows Firewall, BADCALL binds a particular network port (443 or 8000) and listens for incoming connections. Threat actors can connect to the compromised system through this port by generating a fake Transport Layer Security (TLS) handshake using a public Secure Sockets Layer (SSL) certificate from one of several reputable organizations. Threat actors must also supply a specific string of ASCII characters in order to authenticate their connection to BADCALL. If the correct authentication string is not provided, BADCALL immediately terminates the session and responds with a string of unintelligible ASCII characters that indicate the connection was terminated.

Once a threat actor connects and authenticates with BADCALL, the actor can command the malware to begin using the compromised system as a proxy server. Upon receiving this command, BADCALL will attempt to create a proxy session between the threat actor's system and another server. This connection uses a challenge–response authentication model where the proxy server sends the destination server a predetermined ASCII string, and the destination server sends back another predetermined ASCII string. The authentication process ends when both servers have confirmed that they have received the correct string from the other server, at which point they establish a connection with each other.

BADCALL protects its proxy session traffic using a basic rotational cipher based on bitwise XOR and AND operations. When BADCALL filters outgoing bytes through its cipher, the cipher XORs those bytes with the hexadecimal value 47 (47h) and adds the hexadecimal value 28 (28h) to the result. When BADCALL filters incoming bytes through its cipher, the cipher subtracts 28h from those bytes and then XORs the result with 47h, thus reversing the effects of BADCALL's outgoing traffic cipher.

BADCALL also includes a malicious Android Package Kit (APK) that acts as a remote access tool (RAT) for Android-based systems such as smartphones and tablets. When installed it is able to record phone calls made by the device, capture screenshots, use the device's embedded camera, read any contact information stored on the device, and transfer files to and from the device. The BADCALL RAT can also execute commands on the compromised device and scan for open Wi-Fi channels in the device's vicinity.

Prevention and Mitigation

The Cybersecurity and Infrastructure Security Agency (CISA) recommends the following mitigation techniques to defend against attacks that use malware similar to BADCALL and ELECTRICFISH. CISA also stresses that it is crucial to review system configuration changes with system owners and administrators before implementing them because users may face unwanted impacts that can damage their business.

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening email attachments, even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on organization workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on organization workstations and servers.
- Scan for and remove suspicious email attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).

- Monitor users’ web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the internet prior to executing.
- Maintain situation awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

Indicators of Compromise (IOCs)

Indicator	Description
d1f3b9372a6be9c02430b6e4526202974179a674ce94fe22028d7212ae6be9e7	BADCALL, Proxy server (32-bit EXE)
4257bb11570ed15b8a15aa3fc051a580eab5d09c2f9d79e4b264b752c8e584fc	BADCALL, Proxy server (32-bit DLL)
93e13ffd2a2f1a13fb9a09de1d98324f75b3f0f8e0c822857ed5ca3b73ee3672	BADCALL, Implant loader (32-bit EXE)
da353b2845a354e1a3f671e4a12198e2c6f57a377d02dfaf90477869041a044f	BADCALL, Decrypted implant (Zip Archive)
91650e7b0833a34abc9e51bff53cc05ef333513c6be038df29929a0a55310d9c	BADCALL, Proxy server (32-bit DLL)
edd2aff8fad0c76021adc74fe3cb3cb1a02913a839ad0f2cf31fdea8b5aa8195	BADCALL, Remote access tool (Android APK)
7cf5d86cc75cd8f0e22e35213a9c051b740bd4667d9879a446f06277782bffd1	ELECTRICFISH, New variant (32-bit EXE)

Endnotes

1. https://www.us-cert.gov/ncas/analysis-reports/ar19-252a
2. https://www.us-cert.gov/ncas/analysis-reports/ar19-252b
3. https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity
4. https://sites.google.com/a/infoblox.com/cyberint-threat-labs/home/publication-repo/20190507_HIDDEN_COBRA_ElectricFish_CTA_Final.pdf?attredirects=0&d=1
5. https://sites.google.com/a/infoblox.com/cyberint-threat-labs/home/publication-repo/20190410_HIDDEN_COBRA_CTA_Endnotes.pdf?attredirects=0&d=1
6. https://sites.google.com/a/infoblox.com/cyberint-threat-labs/home/publication-repo/20181006_HIDDEN_COBRA_CTA_Endnotes.pdf?attredirects=0&d=1
7. https://sites.google.com/a/infoblox.com/cyberint-threat-labs/home/publication-repo/20180809_CTA_KEYMARBLE_Endnotes.pdf?attredirects=0&d=1
8. https://sites.google.com/a/infoblox.com/cyberint-threat-labs/home/publication-repo/20180618_CTA_Typeframe%20%282%29.pdf?attredirects=0&d=1
9. https://sites.google.com/a/infoblox.com/cyberint-threat-labs/home/publication-repo/CTA-2018-001%20Brambul%20Worm%20%26%20Joanap%20RAT%20%282%29.pdf?attredirects=0&d=1
10. https://sites.google.com/a/infoblox.com/cyberint-threat-labs/home/publication-repo/CTA-2017-004_HiddenCobra.pdf?attredirects=0&d=1

Infoblox
NEXT LEVEL NETWORKING

Infoblox enables next level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world’s most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com