HIDDEN COBRA – North Korean Remote Administration Tool: FALLCHILL | CISA

Published: 2017-11-22 · Archived: 2026-04-05 15:24:06 UTC

Systems Affected

Network systems

Overview

This joint Technical Alert (TA) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). Working with U.S. government partners, DHS and FBI identified Internet Protocol (IP) addresses and other indicators of compromise (IOCs) associated with a remote administration tool (RAT) used by the North Korean government—commonly known as FALLCHILL. The U.S. Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA. For more information on HIDDEN COBRA activity, visit https://www.us-cert.gov/hiddencobra.

FBI has high confidence that HIDDEN COBRA actors are using the IP addresses—listed in this report's IOC files—to maintain a presence on victims' networks and to further network exploitation. DHS and FBI are distributing these IP addresses to enable network defense and reduce exposure to any North Korean government malicious cyber activity.

This alert includes IOCs related to HIDDEN COBRA, IP addresses linked to systems infected with FALLCHILL malware, malware descriptions, and associated signatures. This alert also includes suggested response actions to the IOCs provided, recommended mitigation techniques, and information on reporting incidents. If users or administrators detect activity associated with the FALLCHILL malware, they should immediately flag it, report it to the DHS National Cybersecurity and Communications Integration Center (NCCIC) or the FBI Cyber Watch (CyWatch), and give it the highest priority for enhanced mitigation.

For a downloadable copy of IOCs, see:

- IOCs (.csv)
- IOCs (.stix)

NCCIC conducted analysis on two samples of FALLCHILL malware and produced a Malware Analysis Report (MAR). MAR-10135536-A examines the tactics, techniques, and procedures observed in the malware. For a downloadable copy of the MAR, see:

- MAR (.pdf)
- MAR IOCs (.stix)

According to trusted third-party reporting, HIDDEN COBRA actors have likely been using FALLCHILL malware since 2016 to target the aerospace, telecommunications, and finance industries. The malware is a fully functional

RAT with multiple commands that the actors can issue from a command and control (C2) server to a victim's system via dual proxies. FALLCHILL typically infects a system as a file dropped by other HIDDEN COBRA malware or as a file downloaded unknowingly by users when visiting sites compromised by HIDDEN COBRA actors. HIDDEN COBRA actors use an external tool or dropper to install the FALLCHILL malware-as-a-service to establish persistence. Because of this, additional HIDDEN COBRA malware may be present on systems compromised with FALLCHILL.

During analysis of the infrastructure used by FALLCHILL malware, the U.S. Government identified 83 network nodes. Additionally, using publicly available registration information, the U.S. Government identified the countries in which the infected IP addresses are registered.

Technical Details

FALLCHILL is the primary component of a C2 infrastructure that uses multiple proxies to obfuscate network traffic between HIDDEN COBRA actors and a victim's system. According to trusted third-party reporting, communication flows from the victim's system to HIDDEN COBRA actors using a series of proxies as shown in figure 1.

Figure 1. HIDDEN COBRA Communication Flow

FALLCHILL uses fake Transport Layer Security (TLS) communications, encoding the data with RC4 encryption with the following key: [0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 82]. FALLCHILL collects basic system information and beacons the following to the C2:

- operating system (OS) version information,
- processor information,
- system name,
- local IP address information,
- unique generated ID, and
- media access control (MAC) address.

FALLCHILL contains the following built-in functions for remote operations that provide various capabilities on a victim's system:

- retrieve information about all installed disks, including the disk type and the amount of free space on the disk;
- create, start, and terminate a new process and its primary thread;
- search, read, write, move, and execute files;
- get and modify file or directory timestamps;
- change the current directory for a process or file; and
- delete malware and artifacts associated with the malware from the infected system.

Detection and Response

This alert's IOC files provide HIDDEN COBRA indicators related to FALLCHILL. DHS and FBI recommend that network administrators review the information provided, identify whether any of the provided IP addresses fall within their organizations' allocated IP address space, and—if found—take necessary measures to remove the malware.

When reviewing network perimeter logs for the IP addresses, organizations may find instances of these IP addresses attempting to connect to their systems. Upon reviewing the traffic from these IP addresses, system owners may find some traffic relates to malicious activity and some traffic relates to legitimate activity.

Network Signatures and Host-Based Rules

This section contains network signatures and host-based rules that can be used to detect malicious activity associated with HIDDEN COBRA actors. Although created using a comprehensive vetting process, the possibility of false positives always remains. These signatures and rules should be used to supplement analysis and should not be used as a sole source of attributing this activity to HIDDEN COBRA actors.

Network Signatures

```
alert tcp any any -> any any (msg:"Malicious SSL 01 Detected";content:"|17 03 01 00 08|";
pcre:"/\x17\x03\x01\x00\x08.{4}\x04\x88\x4d\x76/"; rev:1; sid:2;)
```

```
alert tcp any any -> any any (msg:"Malicious SSL 02 Detected";content:"|17 03 01 00 08|";
pcre:"/\x17\x03\x01\x00\x08.{4}\x06\x88\x4d\x76/"; rev:1; sid:3;)
```

```
alert tcp any any -> any any (msg:"Malicious SSL 03 Detected";content:"|17 03 01 00 08|";
pcre:"/\x17\x03\x01\x00\x08.{4}\xb2\x63\x70\x7b/"; rev:1; sid:4;)
```

```
alert tcp any any -> any any (msg:"Malicious SSL 04 Detected";content:"|17 03 01 00 08|";
pcre:"/\x17\x03\x01\x00\x08.{4}\xb0\x63\x70\x7b/"; rev:1; sid:5;)
```

YARA Rules

The following rules were provided to NCCIC by a trusted third party for the purpose of assisting in the identification of malware associated with this alert.

THIS DHS/NCCIC MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. These rules have been tested and determined to function effectively in a lab environment, but we have no way of knowing if they may function differently in a production network. Anyone using these rules are encouraged to test them using a data set representitive of their environment.

```
rule rc4_stack_key_fallchill
{
meta:
    description = "rc4_stack_key"
strings:
    $stack_key = { 0d 06 09 2a ?? ?? ?? ?? 86 48 86 f7 ?? ?? ?? ?? 0d 01 01 01 ?? ?? ?? ?? 05 00 03
82 41 8b c9 41 8b d1 49 8b 40 08 48 ff c2 88 4c 02 ff ff c1 81 f9 00 01 00 00 7c eb }
condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and $stack_key
}

rule success_fail_codes_fallchill

{
meta:
    description = "success_fail_codes"
strings:
    $s0 = { 68 7a 34 12 00 }
    $s1 = { ba 7a 34 12 00 }
    $f0 = { 68 5c 34 12 00 }
    $f1 = { ba 5c 34 12 00 }
condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and (($s0 and $f0) or ($s1 and $f1))
}
```

Impact

A successful network intrusion can have severe impacts, particularly if the compromise becomes public and sensitive information is exposed. Possible impacts include:

- temporary or permanent loss of sensitive or proprietary information,
- disruption to regular operations,
- financial losses incurred to restore systems and files, and
- potential harm to an organization’s reputation.

Solution

Mitigation Strategies

DHS recommends that users and administrators use the following best practices as preventive measures to protect their computer networks:

- Use application whitelisting to help prevent malicious software and unapproved programs from running. Application whitelisting is one of the best security strategies as it allows only specified programs to run, while blocking all others, including malicious software.
- Keep operating systems and software up-to-date with the latest patches. Vulnerable applications and operating systems are the target of most attacks. Patching with the latest updates greatly reduces the number of exploitable entry points available to an attacker.
- Maintain up-to-date antivirus software, and scan all software downloaded from the Internet before executing.
- Restrict users' abilities (permissions) to install and run unwanted software applications, and apply the principle of "least privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through the network.
- Avoid enabling macros from email attachments. If a user opens the attachment and enables macros, embedded code will execute the malware on the machine. For enterprises or organizations, it may be best to block email messages with attachments from suspicious sources. For information on safely handling email attachments, see Recognizing and Avoiding Email Scams. Follow safe practices when browsing the web. See Good Security Habits and Safeguarding Your Data for additional details.
- Do not follow unsolicited web links in emails. See Avoiding Social Engineering and Phishing Attacks for more information.

Response to Unauthorized Network Access

- **Contact DHS or your local FBI office immediately.** To report an intrusion and request resources for incident response or technical assistance, contact CISA Central (SayCISA@cisa.dhs.gov ✉ or by phone at 1-844-Say-CISA), FBI through a local field office, or the FBI's Cyber Division (CyWatch@fbi.gov or 855-292-3937).

Revisions

November 14, 2017: Initial version
