HIDDEN COBRA – Joanap Backdoor Trojan and Brambul Server Message Block Worm | CISA

Published: 2018-05-31 · Archived: 2026-04-05 15:26:33 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 two families of malware used by the North Korean government:

- a remote access tool (RAT), commonly known as Joanap; and
- a Server Message Block (SMB) worm, commonly known as Brambul.

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 enable network exploitation. DHS and FBI are distributing these IP addresses and other IOCs to enable network defense and reduce exposure to any North Korean government malicious cyber activity.

This alert also includes suggested response actions to the IOCs provided, recommended mitigation techniques, and information on how to report incidents. If users or administrators detect activity associated with these malware families, 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.

See the following links for a downloadable copy of IOCs:

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

NCCIC conducted analysis on four malware samples and produced a Malware Analysis Report (MAR). MAR-10135536.3 – RAT/Worm examines the tactics, techniques, and procedures observed in the malware. Visit MAR-10135536.3 – HIDDEN COBRA RAT/Worm for the report and associated IOCs.

According to reporting of trusted third parties, HIDDEN COBRA actors have likely been using both Joanap and Brambul malware since at least 2009 to target multiple victims globally and in the United States—including the

media, aerospace, financial, and critical infrastructure sectors. Users and administrators should review the information related to Joanap and Brambul from the Operation Blockbuster Destructive Malware Report [1] in conjunction with the IP addresses listed in the .csv and .stix files provided within this alert. Like many of the families of malware used by HIDDEN COBRA actors, Joanap, Brambul, and other previously reported custom malware tools, may be found on compromised network nodes. Each malware tool has different purposes and functionalities.

Joanap malware is a fully functional RAT that is able to receive multiple commands, which can be issued by HIDDEN COBRA actors remotely from a command and control server. Joanap typically infects a system as a file dropped by other HIDDEN COBRA malware, which users unknowingly downloaded either when they visit sites compromised by HIDDEN COBRA actors, or when they open malicious email attachments.

During analysis of the infrastructure used by Joanap malware, the U.S. Government identified 87 compromised network nodes. The countries in which the infected IP addresses are registered are as follows:

• **Argentina** • **Belgium** • **Brazil** • **Cambodia** • **China** • **Colombia**	• **Egypt** • **India** • **Iran** • **Jordan** • **Pakistan** • **Saudi Arabia**	• **Spain** • **Sri Lanka** • **Sweden** • **Taiwan** • **Tunisia**

Malware often infects servers and systems without the knowledge of system users and owners. If the malware can establish persistence, it could move laterally through a victim’s network and any connected networks to infect nodes beyond those identified in this alert.

Brambul malware is a brute-force authentication worm that spreads through SMB shares. SMBs enable shared access to files between users on a network. Brambul malware typically spreads by using a list of hard-coded login credentials to launch a brute-force password attack against an SMB protocol for access to a victim’s networks.

Technical Details

Joanap

Joanap is a two-stage malware used to establish peer-to-peer communications and to manage botnets designed to enable other operations. Joanap malware provides HIDDEN COBRA actors with the ability to exfiltrate data, drop and run secondary payloads, and initialize proxy communications on a compromised Windows device. Other notable functions include

- file management,
- process management,
- creation and deletion of directories, and
- node management.

Analysis indicates the malware encodes data using Rivest Cipher 4 encryption to protect its communication with HIDDEN COBRA actors. Once installed, the malware creates a log entry within the Windows System Directory in a file named mssscardprv.ax. HIDDEN COBRA actors use this file to capture and store victims' information such as the host IP address, host name, and the current system time.

Brambul

Brambul malware is a malicious Windows 32-bit SMB worm that functions as a service dynamic link library file or a portable executable file often dropped and installed onto victims' networks by dropper malware. When executed, the malware attempts to establish contact with victim systems and IP addresses on victims' local subnets. If successful, the application attempts to gain unauthorized access via the SMB protocol (ports 139 and 445) by launching brute-force password attacks using a list of embedded passwords. Additionally, the malware generates random IP addresses for further attacks.

Analysts suspect the malware targets insecure or unsecured user accounts and spreads through poorly secured network shares. Once the malware establishes unauthorized access on the victim's systems, it communicates information about victim's systems to HIDDEN COBRA actors using malicious email addresses. This information includes the IP address and host name—as well as the username and password—of each victim's system. HIDDEN COBRA actors can use this information to remotely access a compromised system via the SMB protocol.

Analysis of a newer variant of Brambul malware identified the following built-in functions for remote operations:

- harvesting system information,
- accepting command-line arguments,
- generating and executing a suicide script,
- propagating across the network using SMB,
- brute forcing SMB login credentials, and
- generating Simple Mail Transport Protocol email messages containing target host system information.

Detection and Response

This alert's IOC files provide HIDDEN COBRA IOCs related to Joanap and Brambul. 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.

Impact

A successful network intrusion can have severe impacts, particularly if the compromise becomes public. 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:

- Keep operating systems and software up-to-date with the latest patches. Most attacks target vulnerable applications and operating systems. 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.
- Scan for and remove suspicious email attachments. If a user opens a malicious attachment and enables macros, embedded code will execute the malware on the machine. Enterprises and organizations should consider blocking email messages from suspicious sources that contain attachments. For information on safely handling email attachments, see Using Caution with Email Attachments. Follow safe practices when browsing the web. See Good Security Habits and Safeguarding Your Data for additional details.
- Disable Microsoft's File and Printer Sharing service, if not required by the user's organization. If this service is required, use strong passwords or Active Directory authentication. See Choosing and Protecting Passwords for more information on creating strong passwords.
- Enable a personal firewall on organization workstations and configure it to deny unsolicited connection requests.

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 FBI's Cyber Division (CyWatch@fbi.gov or 855-292-3937).

References

[1] Novetta's Destructive Malware Report

Revisions

May 29, 2018: Initial version|May 31, 2018: Uploaded updated STIX and CSV files

Source: https://www.us-cert.gov/ncas/alerts/TA18-149A