HIDDEN COBRA – North Korean Trojan: Volgmer | CISA

Published: 2017-11-22 · Archived: 2026-04-05 13:39:18 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 Trojan malware variant used by the North Korean government—commonly known as Volgmer. 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 North Korean government malicious cyber activity.

This alert includes IOCs related to HIDDEN COBRA, IP addresses linked to systems infected with Volgmer 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 Volgmer 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 five files associated with or identified as Volgmer malware and produced a Malware Analysis Report (MAR). MAR-10135536-D examines the tactics, techniques, and procedures observed. For a downloadable copy of the MAR, see:

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

Volgmer is a backdoor Trojan designed to provide covert access to a compromised system. Since at least 2013, HIDDEN COBRA actors have been observed using Volgmer malware in the wild to target the government, financial, automotive, and media industries.

It is suspected that spear phishing is the primary delivery mechanism for Volgmer infections; however, HIDDEN COBRA actors use a suite of custom tools, some of which could also be used to initially compromise a system.

Therefore, it is possible that additional HIDDEN COBRA malware may be present on network infrastructure compromised with Volgmer

The U.S. Government has analyzed Volgmer's infrastructure and have identified it on systems using both dynamic and static IP addresses. At least 94 static IP addresses were identified, as well as dynamic IP addresses registered across various countries. The greatest concentrations of dynamic IPs addresses are identified below by approximate percentage:

- India (772 IPs) 25.4 percent
- Iran (373 IPs) 12.3 percent
- Pakistan (343 IPs) 11.3 percent
- Saudi Arabia (182 IPs) 6 percent
- Taiwan (169 IPs) 5.6 percent
- Thailand (140 IPs) 4.6 percent
- Sri Lanka (121 IPs) 4 percent
- China (82 IPs, including Hong Kong (12)) 2.7 percent
- Vietnam (80 IPs) 2.6 percent
- Indonesia (68 IPs) 2.2 percent
- Russia (68 IPs) 2.2 percent

Technical Details

As a backdoor Trojan, Volgmer has several capabilities including: gathering system information, updating service registry keys, downloading and uploading files, executing commands, terminating processes, and listing directories. In one of the samples received for analysis, the US-CERT Code Analysis Team observed botnet controller functionality.

Volgmer payloads have been observed in 32-bit form as either executables or dynamic-link library (.dll) files. The malware uses a custom binary protocol to beacon back to the command and control (C2) server, often via TCP port 8080 or 8088, with some payloads implementing Secure Socket Layer (SSL) encryption to obfuscate communications.

Malicious actors commonly maintain persistence on a victim's system by installing the malware-as-a-service. Volgmer queries the system and randomly selects a service in which to install a copy of itself. The malware then overwrites the ServiceDLL entry in the selected service's registry entry. In some cases, HIDDEN COBRA actors give the created service a pseudo-random name that may be composed of various hardcoded words.

Detection and Response

This alert's IOC files provide HIDDEN COBRA indicators related to Volgmer. 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:"Malformed_UA"; content:"User-Agent: Mozillar/"; depth:500; sid:99999999;)
```

YARA Rules

```
rule volgmer
{
meta:
    description = "Malformed User Agent"
strings:
    $s = "Mozillar/"
condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and $s
}
```

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
