Mariposa Botnet | CISA

Published: 2014-01-20 · Archived: 2026-04-05 19:45:17 UTC

Overview

ICS-CERT has received reports and investigated infections of the MariposaDefence Intelligence, http://defintel.com/docs/MariposaAnalysis.pdf, website last accessed March 15, 2010. botnet, which have affected the business networks of multiple control system owners in recent months.

ICS-CERT has no information to indicate that these infections have specifically targeted United States Critical Infrastructure and Key Resources (CIKR), or any specific sector or organization.

Background

In May 2009, Defence Intelligence announced the discovery of a botnet, called “Mariposa.” An investigation followed this discovery and targeted bringing down the criminal network behind what has become one of the largest botnets on record.

After months of investigation by the Guardia Civil in Spain, the FBI, security firm Panda Security, and Defence Intelligence, authorities took down a 12.7 million strong zombie network in December. In February 2010, Spanish authorities arrested three suspects in Spain.John Leyden, http://www.theregister.co.uk/2010/03/04/mariposapolicehuntmorebotherders/, website last accessed March 15, 2010.

Although the primary command and control (C2) infrastructure for the Mariposa botnet is considered to have been rendered inoperative by the Mariposa Working Group,PandaLabs, http://pandalabs.pandasecurity.com/mariposa-botnet/, website last accessed March 15, 2010. malware files that were used by the botnet are still thought to be on computers in production environments and should be identified and removed. Additionally, it is not uncommon for new groups to assume control of old or abandoned botnets by compromising existing command and control or by establishing new command and control infrastructure using slightly modified malware.

Details

In February 2010, a US utility company (USUTIL1) was notified by another US Utility partner company (USUTIL2) that a USUTIL1 employee had visited USUTIL2 with a Mariposa-infected laptop. There had been no indication from USUTIL1’s computer network defense mechanisms (Anti-Virus, Intrusion Detection Systems, Firewalls etc.) that an infection had occurred and USUTIL2’s notification was USUTIL1’s first indication that there was an issue.

USUTIL1’s investigation found that the initial infection vector may have been a USB drive shared at an industry conference. An instructor shared a USB drive among participants at a training event attended by USUTIL1’s

employee. It is believed that when the employee returned and connected his laptop to the corporate network, the malware spread to multiple business systems.

To date, none of USUTIL1's control systems are known to be affected by the botnet malware.

USUTIL1's internal investigation found the malware file "Schl.exe" in deleted files on one system. USUTIL1's continued searching and found other systems with this deleted file. These systems were also attempting to make UDP connections with systems outside of their firewall.

ICS-CERT was contacted and at the request of the organization, deployed a fly-away team to assist with identification and analysis of the malware.

Analysis

A dynamic analysis was made on the file schl.exe. The method used for code injection is similar to the method described by Defence IntelligenceDefence Intelligence, http://defintel.com/docs/MariposaAnalysis.pdf, website last accessed March 15, 2010. however, callbacks appeared to be unique. It should be noted that the following information is solely from ICS-CERT's investigation into the malware variant found at USUTIL1. This information, along with other open source information should be leveraged in any comprehensive detection and mitigation activities.

The following information can be used to develop detection signatures:

File: SCHL.EXE

Size: 140800
MD5: 645C4DD7508B3DC83807FCF9918FE1C7
SHA1: d452e2df58fad206b2213683356033822ff335c9
Type: PE32 executable for MS Windows (GUI) Intel 80386 32-bit

Antivirus Identification

Microsoft: Trojan:Win32/Meredrop
Mcafee: Backdoor-EEC.gen
Symantec: Trojan Horse

DNS Lookups

hnox[dot]org
socksa[dot]com
ronpc[dot]net

Callbacks

Domain	IP	Protocol/Port
hnox[dot]org	92.241.165.162	UDP 21039
socksa[dot]com	92.241.164.82	UDP 21039
ronpc[dot]net	*92.241.164.82*	*UDP 21039*

Note: All network traffic in/out is UDP

The initial outbound packet is 49 bytes (7 bytes encrypted payload) to hnox[dot]org or socksa[dot]com, using UDP port 21039, for the purpose of establishing the C2 channel. The C2 server responds from 21039 to the same local port, with a UDP packet of varying length and encrypted payload. C2 command syntax appears to be consistent with the Mariposa botnet.

Malware Files

schl.exe – dropper
jack.exe – dropped file
config.inf – dropped file
desktop.ini – dropped file (0-byte file located at source of originally executed file)

Botnets, including Mariposa, are highly dynamic. C2 operators frequently update their code to evade detection or implement new features. Other files may also be associated with Mariposa, so the list above is not a complete list of files used by Mariposa. For example, Defence IntelligenceeDefence Intelligence, http://defintel.com/docs/MariposaAnalysis.pdf, website last accessed March 15, 2010. has also identified blackjackson.exe, which provided Mariposa with distributed denial-of-service (DDoS) capability by using the BlackEnergy DDoS bot.

Windows Registry Modifications

Key: [HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon]
Value: "Taskman" = "<file_path>\schl.exe"

Note: Where "file path" = location of schl.exe when executed

Domain Names Observed as C2 Servers

The following domain names have been observed as command and control servers:

- bf2back.sinip.es
- bfisback.no-ip.org
- bfisback.sinip.es
- binaryfeed.in
- booster.estr.es
- butterfly.BigMoney.biz

- butterfly.sinip.es
- defintelsucks.com
- defintelsucks.net
- defintelsucks.sinip.es
- extraperlo.biz
- gusanodeseda.mobi
- gusanodeseda.net
- gusanodeseda.sinip.es
- lalundelau.sinip.es
- legion.sinip.es
- legionarios.servecounterstrike.com
- mierda.notengodominio.com
- qwertasdfg.sinip.es
- sexme.in
- shv4.no-ip.biz
- shv4b.getmyip.com
- tamiflux.net
- tamiflux.org
- thejacksonfive.biz
- thejacksonfive.mobi
- thejacksonfive.us
- thesexydude.com
- youare.sexidude.com
- yougotissuez.com

ICS-CERT Identified Malware Files

ICS-CERT identified the following three malware files during analysis:

- schl.exe
- jack.exe
- config.inf

Outbound Command & Control Attempts

ICS-CERT observed attempted UDP C2 connections with the following IP addresses:

- 24.173.86.145
- 67.210.170.32
- 92.241.165.162
- 62.128.52.191
- 74.208.162.142
- 200.74.244.84
- 66.197.176.41

- 76.73.56.12
- 204.16.173.30
- 67.210.170.131
- 87.106.179.75

Mariposa M alware UDP Ports

Mariposa malware has been observed using the following UDP ports:

- 3431
- 3435
- 5907
- 3433
- 3437
- 21039
- 3434
- 5906

Affected Operating Systems

Although botnet malware can affect any operating system, most current botnets including Mariposa target Windows systems.Zeng, Hu, & Shin, “Detection of Botnets Using Combined Host- and Network-Level Information,” 16th ACM Conference on Computer and Communications Security, November 2009:2.

Impact

Although the primary Mariposa C2 is believed to be inactive, the malware is still spreading. The possibility exists that another actor will attempt to “commandeer” the existing C2 or create a new C2 infrastructure. Without C2 direction, the malware won’t perform malicious actions; however, the malware still presents a risk and any remaining Mariposa malware should be identified, removed, and systems should be properly re-imaged or restored if re-imaging is not feasible.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

Recommendations

Because IP addresses, UDP ports, and domains used by the C2 structure of Mariposa changed continually, it created a difficult challenge for security administrators to mitigate the capabilities of this botnet. The best mitigation strategy is to track down compromised systems using all information available about the malware. Organizations should establish firewall rules to block communication from malware to known command and control sites and monitor their network for this activity to identify compromised machines. Additionally, UDP connections are used for Mariposa communication, so observance of your network activity is the best place to

start. If one system is frequently sending outbound UDP packets, regardless of port, mark it as suspicious and investigate the source of the traffic on the system.

It is important to identify all of the infected machines and to disable them simultaneously to prevent re-infection of your assets. Advanced threats such as botnets can be extremely difficult to eradicate. If a compromised system is missed, the threat can re-infect “clean” systems. Clean systems should be isolated while the remainder of the network is cleaned, or the clean systems risk being re-infected. In large networks, this can be a challenging exercise.

As mentioned, IP addresses, ports, and domains used by Mariposa’s C2 system have continually changed. These changes created new malware variants (mariposa had over 1,500 variants) resulting in a persistent and dynamic botnet. It is important to use all available information when eradicating and defending against a botnet infection to ensure that all variants are detected and properly removed.
Here are some general guidelines for dealing with Mariposa malware:

- Any infected systems should be immediately isolated from the network.
- Any systems sharing network drives with the infected systems, including file servers hosting said network drives, should also be isolated from the network.Reimage infected hosts prior to returning to normal operation.
- Consider maintaining an infected system for more detailed analysis (i.e., digital media analysis, malware collection).
- Review antivirus software specific removal guidelines for the malware if re-imaging is not possible.
- Users should refrain from or be administratively prohibited from browsing the Internet using Windows accounts with Administrator-level privileges. This reduces the potential damage an infection can inflict upon a system.
- Organizations should warn users about the risks of using USB drives on business systems. For more information, review *ICS-CERT CSAR -10-090-01- USBs Used as Attack Vectorg and US-CERT Cyber Security Tip ST08-001, “Using Caution with USB Drives*.”US-CERT Cyber Security Tip, http://www.us-cert.gov/cas/tips/ST08-001html, website last accessed March 15, 2010.
- Keep systems up to date with the latest patches and antivirus signatures.
- Establish an internet proxy service and monitor it for suspicious activity.
- Monitor IDS/IPS solutions for connections to the malicious domains and IP addresses listed in ICS-CERT advisories and US-CERT CIINs.
- Do NOT trust unsolicited e-mail.
- Do NOT click links and attachments in unsolicited e-mail messages.
- Employ the use of a spam filter.
- To educate users about social engineering and phishing attacks, review *US-CERT Cyber Security Tip ST04-014, “Avoiding Social Engineering and Phishing Attacks*.”
- To learn more about botnets, review *US-CERT Cyber Security Tip ST06-001, “Understanding Hidden Threats: Rootkits and Botnets*."