

[REVS] Sinit P2P Trojan Analysis

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0024.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 12/08/03

To: list@securiteam.com

Date: 8 Dec 2003 10:41:02 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Sinit P2P Trojan Analysis

SUMMARY

A common tactic among Trojan writers is the multi-stage install. A compact, single-purpose piece of malware gains a foothold on a system then downloads additional components from hidden websites or FTP server. This allows the Trojan writer additional flexibility in being able to update the functionality of the Trojan system from one location. Probably the most prevalent example of this type of attack can be seen in the Sobig family of email worms. The primary problem with this approach is the single point of failure – once the download site is discovered, it is usually shut down in short order. Later variants of Sobig attempted to solve this problem by establishing an encrypted communication with an intermediary layer of 20 hosts that would point it to the real download site. This approach was only successful for a short time; eventually law enforcement became involved with shutting the intermediary hosts and downloads sites down, and was largely successful at preventing the last variant of Sobig from downloading anything at all.

DETAILS

The P2P Concept:

The next logical step in the evolution of the "downloader" Trojan is the peer-to-peer distribution model. This eventuality has now been realized in

Securiteam: [REVS] Sinit P2P Trojan Analysis

the Trojan known as Backdoor.Sinit (a.k.a. Calyps.a or Calypso). With Sinit, there is no central server that can be shut down. Each infected host becomes part of a peer-to-peer network through which additional Trojans are spread to all hosts. Code can be injected at any point in the network and it will eventually be copied to all hosts. As an additional improvement, the Trojans being copied over the P2P network are digitally signed to prevent corruption or "foreign" code from being introduced. Only the person(s) holding the correct private encryption key will be able to spread new files to the infected hosts.

Most peer-to-peer networks have some concept of a central server or "seed lists" of peers who can be contacted in order to join the network. While this is not a major problem for the typical P2P network, it again represents a single point of failure for the Trojan P2P network. The alternative is to send out packets to random destinations until you establish a list of peers with which you can communicate. This is exactly how Sinit works, although it tries to limit the targeted IP ranges to sane values.

The packets Sinit uses in its discovery protocol were detected quickly by users of intrusion detection systems. These packets are sent over UDP port 53, but are not DNS protocol packets. Because IDS systems often check this port/protocol for sanity, reports of widespread "malformed DNS packets" were everywhere. At first this traffic was theorized to be part of some massive DNS fingerprinting effort, but eventually it was realized that Sinit was the culprit. However, the purpose of the packets (and Sinit itself) was still not understood.

How It Works:

The Sinit Trojan has a communication protocol based on six types of packets, each one prefixed with a byte of value 1-6 and maximum size of 512 bytes. It listens on UDP port 53 and also a high-numbered random UDP port. Either port will respond to the protocol packets described below:

0x01 – Discovery – The discovery packet is used to establish the initial communication with other infected clients. If the sending host has information about other infected hosts it will be sent in this packet as well, along with the timestamp of the most recent malware that has been pushed to it. Upon receiving this packet, infected hosts will respond with the 0x05 packet, and may share the list of hosts they know about or push additional malware to systems who are not up-to-date.

0x02 – Status – These packets are sent with a payload which indicates the status of a file transfer.

0x03 – File Transfer – These packets contain information indicating the offset of the data in the file being transferred along with the data from the file.

0x04 – File Request – This packet is used by Sinit to request a file transfer from a remote host who has newer malware available.

Securiteam: [REVS] Sinit P2P Trojan Analysis

0x05 – Discovery Response – This packet is sent in reply to the 0x01 packet, and will contain the IP address and port of the host that sent the first packet. When the 0x05 packet arrives back at the first host, Sinit attempts to bind a socket to the IP address in the packet. This allows Sinit to detect whether it is behind a NAT device, or possibly on a multi-homed system. If the bind is successful and the IP address is different than what Sinit thinks is the current system IP address, it will begin sending this "external" address in future discovery (0x01) packets.

0x06 – EOF – This packet is sent at the end of a file transfer to indicate the transfer is complete.

Additional Functionality:

There is a 412-byte header added to each executable or DLL file transferred. This header contains the timestamp of the file which is converted to a system filename using an alphabetic substitution cipher and stored in the Windows system directory as a .TMP file. The header also contains two digital signatures, one for the embedded executable code and one for the header itself. The header signature is checked when the first 0x03 packet is sent, and the file signature is checked when the transfer is complete. If the first check fails the transfer is aborted. If the second check fails, the file is deleted from memory before being copied to the filesystem. If the checks are successful, the embedded file is copied to the filesystem. If the file is executable, it is launched as a separate process. If the file is a .DLL it is loaded into the memory space of Sinit and the "Init" function of the .DLL is called.

Sinit also listens on TCP port 53, and acts as a webserver in a limited way. Its only function is to distribute its own code to uninfected hosts, presumably by way of a browser exploit. Since the Sinit Trojan itself is distributed from infected hosts there is again no central download site that can be shut down to prevent it from being downloaded during the exploit phase. One positive side-effect of distributing the code this way is that it is easy for virus researchers to obtain new samples of the code remotely from the infected hosts, and it is easy to tell who is infected with the Trojan and what variant they are infected with. One merely needs to request the file using the following URL:

[http:// address of infected host:53/kx.exe](http://address of infected host:53/kx.exe)

On a random DSL subnet we checked, there were two infected hosts out of the possible 253 IP addresses. Based on this unscientific sample, we would guess that the total number of infected hosts is easily in the tens or hundreds of thousands worldwide. The real number could be far more, but it is almost certainly not less.

Origins:

Various files have been observed traversing the Sinit network. One of these files has been linked to CoolWebSearch, a family of Trojans which hijack browser settings for the purpose of popping up ads or redirecting an unsuspecting user's traffic to questionable sites. The CoolWebSearch

Securiteam: [REVS] Sinit P2P Trojan Analysis

Chronicles, a site which has been tracking the variants of this Trojan for some time, has also made the connection between Sinit and CoolWebSearch. They theorize that the initial infection is made via an Internet Explorer browser exploit known as Java-ByteVerify. Also "dialers" have been witnessed being downloaded. These are programs which cause your modem to dial expensive pay-per-minute phone numbers in foreign countries. By-and-large Sinit appears to have been created as a money-making endeavor rather than a proof-of-concept.

Removal:

There have been at least four variants of Sinit so far (probably more), the earliest one we have seen was compiled on Mon Sep 29 13:09:17 2003. The earliest variants used the executable name svcinit.exe, but later variants have been known to use the executable name svcpack.exe. With either one you can use the task manager to kill the svcinit or svcpack process, then remove the file from your Windows system directory and remove the HKLM\Software\Microsoft\Windows\CurrentVersion\Run registry key associated with the executable. If you don't feel comfortable editing your registry, you may want to try CWShredder, a free program which can remove all known versions of CoolWebSearch trojans. CWShredder can be found here: <http://www.spywareinfo.com/~merijn/cwschronicles.html>

Summary:

Certainly the most notable aspect of Sinit is the P2P capability. It's like KaZaA only without all the pesky copyrighted files clogging up your Trojan-spreading bandwidth. However, it is interesting (and perhaps ironic) that digitally signed code, which has long been touted as the answer to preventing "bad" code from running on your OS, is now being utilized by the Trojan writers. Finally, this Trojan is also further evidence that money, not notoriety, is now the major driving force behind the spread of malware these days. It's always been an arms race in the virus/anti-virus world, but now both sides have financial incentive to continue the battle.

ADDITIONAL INFORMATION

The original analysis is available from: <http://www.lurhq.com/sinit.html>

The information has been provided by <mailto:jstewart@lurhq.com> Joe Stewart.

=====

This bulletin is sent to members of the SecuriTeam mailing list. To unsubscribe from the list, send mail with an empty subject line and body to: list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.