The maximum classification allowed on GCWiki is **TOP SECRET STRAP1 COMINT**. Click to report inappropriate content.

For GCWiki help contact: [redacted] Support page

SEBACIUM

From GCWiki
(Redirected from File Transfer - FTP)
Jump to: navigation, search

Contents

[edit] Overview

SEBACIUM is the codename for the suite of tools developed as part of ICTR-NE's active P2P exploitation research. These tools fall into 3 categories; monitoring, information operations and effects.

[edit] Monitoring - DIRTY RAT

this tool is aimed at identifying users sharing, downloading or searching for specific content as identified by its customers. P2P traffic represents a large proportion of Internet traffic, the advantages of the SEBACIUM architecture is that it provides a targeted mechanism of obtaining relevant data, regardless of accesses and geographical location.

DIRTY RAT currently has the capability to identify users sharing/downloading files of interest on the eMule (Kademlia) and Bittorrent networks. On eMule it also has the ability to monitor the sharing/downloading of files related to particular keywords. For example, we can report who (IP address and user ID) is sharing files with "jihad" in the filename on eMule. If there is a new publication of an extremist magazine then we can report who is sharing that unique file on the eMule and Bittorrent networks

The capability has proven highly successful and is being used extensively by JTRIG who are in the process of fully integrating it into their systems. DIRTY RAT will soon be delivered to the Metropolitan Police and we are in the early stages of relationships with CEOP and the FBI.

[edit] Information Operations - PLAGUE RAT

This tool has the capability to alter the search results of eMule and deliver tailored content to a target. This capability has been tested successfully on the Internet against ourselves and testing against a real target is being pursued.

[edit] Effects - ROBO RAT

Operationally referred to as ROLLING THUNDER, the details of this tool are UKEO, please contact ICTR-NE (NE distro) for details.

[edit] Future work

Research is continuing to extend the capability to cover the following P2P networks:

- Gnutella currently in prototyping evaluation
- Bittorrent currently in prototyping evaluation. You can help us by identifying torrent files of interest (e.g. extremist material).

We would also like to exploit further a number of opportunities for SEBACIUM to deliver Effects e.g. content delivery attacks, information operations, denial of service and botnet disruption. We are currently pursuing these.

[edit] Tasking

The SEBACIUM system is tasked by keyword(s) that are used to match search/sharing requests on the network.

Although the SEBACIUM system is deployed within JTRIG it is currently still a research prototype, therefore please contact ICTR-NE with any requests that may provide benefit to your business area.

[edit] Classification policy

[edit] Data

- The details of how SEBACIUM works are classified as UK SECRET STRAP2.
- Raw SEBACIUM logs may be distributed at RESTRICTED level, as long as the source of the information and nature of access is not disclosed. The raw logs will contain an IP address of the machine sharing or requesting files of interest, together with a timestamp. Clearly, if this information is

- used in a subscriber check, the identity of the actual owner of the IP address is of a higher classification and should be protected appropriately.
- Results returned by DIRTY RAT are classified as SECRET. The higher classification is given due to the volumes of data and the search criteria used.
- Some filenames, particularly those related to paedophile material, may be particularly offensive. SEBACIUM logs should therefore be distributed to customer departments through secure channels, or the results of analysing those logs incorporated into EPRs.

[edit] Operational prototypes

Although the SEBACIUM techniques are classified, the systems that implement those techniques are considered to be UNCLASSIFIED. This is because they are deployed using covert Internet access, and no targeting or other information is present on the hosting machines that indicate either GCHQ involvement or its interests.

[edit] Interested Parties

(Please feel free to add your team and/or name here)

JTRIG

CBRN

NDIST - Effects

[edit] Notes for SEBACIUM Admins

[edit] Logging

Make sure that log4j has been set to use UTF8 encoding in the properties file for each of the appenders. For example:

```
log4j.appender.A1.encoding=UTF-8
```

[edit] Running

SEBACIUM should be scheduled to run once a day for 24 hours, if run for longer the machine can start to slow down and logging will be affected. This issue is being looked into by QinetiQ and is thought to be a memory related. Make sure you reserve enough memory for the JVM, this amount depends on how much is available and how many hashes are on cover, the minimum is about 400MB, something like 2GB would be preferable.

[edit] Hashing and Topic Files

Please ensure that all topic files are given UNCLASSIFIED names and NO KEYWORDS are placed anywhere on the SEBACIUM box.

When hashing unicode keywords please make sure that unicode has been set up properly on the box and the input/output for all scripts has been explicitly set to use UTF-8. This should be done in DIRTY RAT and there are also some tips on the ICTR-NE code snippets page

When hashing files, be sure that you are using the correct algorithm for eMule MD4 file hashing. This works by hashing ~9MB chunks of the file and then hashing the concatenated result, which is not how the normal MD4 hashing algorithm works. We have a tool provided by QinetiQ to do this and there are also freeware programs available on the Internet, such as:

```
http://slavasoft.com/zip/fsum.zip
```

[edit] File Hash Monitoring

When monitoring file hashes with SEBACIUM you should expect to see logs for KADEMLIA2_PUBLISH_SOURCE_REQ, KAS_ID_LOOKUP and KADEMLIA2_SEARCH_SOURCE_REQ. The KADEMLIA2_SEARCH_SOURCE_REQ packet indicates that the user is downloading the file, if this is not followed by a KADEMLIA2_PUBLISH_SOURCE_REQ for the user then this may indicate that the user is not sharing the files they download from the network.

IMPORTANT: The user hash given by the KAD_ID_LOOKUP is the KADEMLIA hash for a client, whereas the user hash given by the KADEMLIA2_PUBLISH_SOURCE_REQ is the client's eDonkey hash which we are not currently concerned with.

POC: [redacted])

Retrieved from "https://[redacted]

Categories: Applied Research Prototypes | Applied Research | B16 | Peer-to-peer | P2p | Prototypes | SEBACIUM | File Transfer

Views

- Page
- Discussion
- Edit
- History
- Delete
- Move
- Watch
- Additional Statistics

Personal tools

- [redacted]
- My talk
- My preferences
- My watchlist
- My contributions

Navigation

- Main Page
- Help Pages

- Wikipedia Mirror
- Ask Me About...
- Random page
- Recent changes
- Report a Problem
- Contacts
- GCWeb

Search

Go Search

Toolbox

- What links here
- Related changes
- Upload file
- Special pages
- Printable version
- Permanent link

- This page was last modified on 16 July 2010, at 14:36.
- This page has been accessed 1,936 times.
- All material is UK [http://[redacted] Copyright] © 2008 or is held under licence from third parties. This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ [redacted]
- Privacy policy
- About GCWiki
- Disclaimers

SECRET STRAP1 COMINT
The maximum classification allowed on GCWiki is **TOP SECRET STRAP1 COMINT**. Click to report inappropriate content.