MALWARE
INVESTIGATOR

Malware Investigator InfraGard Release Frequently Asked Questions

What is Malware Investigator?

Malware Investigator is an automated system that analyzes suspected malware samples and quickly returns technical information about the samples to its users so they can understand the functionality of the samples. The system, built in cooperation with our federal partners, is an extension of an internal malware analysis tool that the FBI created for its own use in 2011. It proved so successful that the FBI built a version for external partners.Malware Investigator uses an extensive combination of dynamic and static analysis tools to understand how the sample interacts within various types of host environments. It also allows the availability to **correlate** samples and **collaborate** with others, if desired to "connect dots" between cyber events.

Why is Malware Investigator different?

There are four main differences between Malware Investigator and other services that provide some form of automated malware analysis.

1. Each sample uploaded to Malware Investigator provides another data point to help the Federal Bureau of Investigation understand the cyber threat picture, both from a criminal as well as a counterintelligence perspective. This information allows the U.S. Government and its allied partners to more effectively address these cyber threats.

2. Malware Investigator is "tool agnostic." Some organizations offering malware analysis use analytical tools that are created and designed by and for that entity's focus. Malware Investigator was designed to provide the most complete analysis possible by incorporating multiple tools into one system.

3. Malware Investigator does not give or provide information about you and your data to other individuals or entities. The FBI collects Malware samples for its repository in order to understand cyber threats from a macro perspective, and does not track an individual to his or her sample.

4. Malware Investigator provides its user the ability to correlate samples and collaborate with other individuals and organizations as desired. Based on sharing preferences set by users, it correlates current samples with previously submitted identical samples. It also identifies previously submitted samples that are functionally very similar. This information allows Malware Investigator users to link samples together so they can better understand the threat and mitigate it.

FEDERAL BUREAU OF INVESTIGATION

INFRAGARD
PARTNERSHIP FOR PROTECTION

MALWARE
INVESTIGATOR

Who can Access Malware Investigator?

Malware Investigator is available to anyone who maintains a trusted relationship with the FBI.

Current Trusted partners include local, state, other federal, and international law enforcement partners through the Law Enforcement Enterprise Portal (LEEP, formerly LEO) and the National Cyber Forensics & Training Alliance (NCFTA). The FBI is now ready to expand its partnerships by offering it to its private sector partners.

How can a private sector partner access Malware Investigator?

Beginning late February 2015, Malware Investigator will be available through the InfraGard portal. The FBI's InfraGard program is an information sharing and analysis effort combining the knowledge base, and serves the interests of a wide range of private sector partners who own, operate and hold key positions within some 85% of the nation's critical infrastructure. Membership within InfraGard affords access to the FBI's InfraGard portal which provides opportunities for networking and hosts numerous analytical products and tools to include Malware Investigator. To join InfraGard visit https://www.InfraGard.org.

Frequently Asked Questions:

How Do I access Malware Investigator?
InfraGard members wishing to use Malware Investigator must access the iLEEP portal through the InfraGard system. iLEEP requires that those submitting malware are currently employed with a verified organization.

What types of information is provided by Malware Investigator?
Submitters receive a technical report so they can understand the functionality of the malware submitted, the damage it can do, and when sharing is enabled, highlights previous incidents when the malware was seen. Using collaborative sharing features enables the system to "connect the dots" by linking previous seemingly unrelated incidents.

What options do I have for sharing malware?
For privacy reasons, the information sharing option is turned off by default, but users may control sharing by changing the settings within the Account Preferencce tab. Malware Investigator allows users to choose who else can see information about their submitted samples. The settings can be changed at anytime. When samples are shared, others can make correlations between their submissions and the samples that you share. Although default settings restrict sharing for privacy reasons, Malware Investigator works most effectively when its user community shares freely.

What if I'm not an InfraGard Member?
Currently the tool is only available to members of InfraGard through the InfraGard portal. However, the FBI is working to expand the tool's availability. Those wishing to access the tool, and other resources, can become a member of InfraGard by visiting https://www.InfraGard.org. Membership requires an individual to be a U.S. citizen, who are 18 years of age or older to consent and pass an FBI security risk assessment to be affiliated to a critical infrastructure sector, and agree to InfraGard policies.

How do I seek help with problems accessing Malware Investigator?
For assistance with accessing Malware Investigator via the InfraGard Network Portal, please call the InfraGard Network Helpdesk at (877) 861-6298 or email via infragardhelpdesk@leo.gov.

How do I report issues I may have with Malware Investigator?
You may report issues by clicking the **"Need Help?"** link at the bottom of the Malware Investigator page.

FEDERAL BUREAU
OF INVESTIGATION