APPENDIX G (DIGITAL): IOCs

The portion of this appendix that includes the Indicators of Compromise (IOCs) is digital and can be found at http://www.mandiant.com/apt1.

APT1 Indicators and Using Redline™

With the release of Mandiant's report, APT1: Exposing One of China's Cyber Espionage Units, we are providing a set of APT1 IOCs in the digital portion of Appendix G to help detect malware described in Appendix C: The Malware Arsenal. IOCs can be used in investigations to find unknown evils or for detection of already known threats. The IOCs included in Appendix G fit the latter; however, keep in mind that APT1 does update their tools, and there are certainly malware variants and new families of malware that will not be detected with this set of IOCs. To find out more about the report or the digital appendices (to include downloading the set of APT1 IOCs in Appendix G: IOCs) go to http://www.mandiant.com/apt1.

IOCs can be used in conjunction with Redline, Mandiant's free host-based investigative tool, or with Mandiant Intelligent Response® (MIR), Mandiant's commercial host-based investigative tool. Mandiant's customers who have licensed MIR can simply import a zip file of the IOCs into their controllers. For those without MIR, Redline can be downloaded from Mandiant's web site at http://www.mandiant.com/resources/download/redline.

Remember to always test new IOCs before using them in a production environment.

What Are IOCs?

Mandiant has developed an open, extendable standard for defining and sharing threat information in a machine-readable format. Going well beyond static signature analysis, IOCs combine over 500 types of forensic evidence with grouping and logical operators to provide advanced threat detection capability.

If you are not familiar with IOCs, go to the OpenIOC site for a description at http://openioc.org.

What Is Redline?

Redline is Mandiant's free tool for investigating hosts for signs of malicious activity through memory and file analysis, and subsequently developing a threat assessment profile. Redline provides several benefits including the following:

RAPID TRIAGE

When confronted with a potentially compromised host, responders must first assess whether the system has active malware. Without installing software or disrupting the current state of the host, Redline thoroughly audits all currently-running processes and drivers on the system for a quick analysis; for a detailed analysis, it also collects the entire file structure, network state, and system memory. Redline will also compare any MD5 value it collects, analyzes, and visualizes against an MD5 whitelist. Users can further analyze and view imported audit data using Redline's Timeline functionality, which includes capabilities to narrow and filter results around a given timeframe with the TimeWrinkles™ and TimeCrunches™ features.

REVEALS HIDDEN MALWARE

The Redline Portable Agent can collect and analyze a complete memory image, working below the level at which kernel rootkits and other malware-hiding techniques operate. Many hiding techniques become extremely obvious when examined at the physical memory level, making memory analysis a powerful tool for finding malware. It also reveals "memory only" malware that is not present on disk.

GUIDED ANALYSIS

Mandiant's Redline tool streamlines memory analysis by providing a proven workflow for analyzing malware based on relative priority. This takes the guesswork out of task and time allocation, allowing investigators to provide a focused response to the threats that matter most.

Redline calculates a "Malware Risk Index" that highlights processes more likely to be worth investigating, and encourages users to follow investigative steps that suggest how to start. As users review more audits from clean and compromised systems, they build up the experience to recognize malicious activity more quickly.

As you investigate a system, here's how Redline will help you focus your attention on the most productive data:

INVESTIGATIVE STEPS

Redline can collect a daunting amount of raw information. Its investigative steps help provide a starting place by highlighting specific data and providing views that are most commonly productive in identifying malicious processes. Unless you are pursuing a specific "lead", we recommend working through the steps in order, examining the information for entries that don't match your expectations.

The key to becoming an effective investigator is to review Redline data from a variety of "clean" and "compromised" systems. Over time, your sense of which entries are normal and which are of concern will develop quickly as you view more data.

MALWARE RISK INDEX SCORING

Redline analyzes each process and memory section using a variety of rules and techniques to calculate a "Malware Risk Index" for each process. This score is a helpful guide to identifying those processes that are more likely to be worth investigating. Processes at the highest risk of being compromised by malware are highlighted with a red badge. Those with some risk factors have a grey badge, and low-risk processes have no badge.

The MRI is not an absolute indication of malware. During an investigation you can refine the MRI scoring by adjusting specific hits (identifying false positives and false negatives) for each process, adding your own hits, and generally tuning the results.

IOCs

Redline provides the option of performing IOC analysis in addition to MRI scoring. Supplied a set of IOCs, the Redline Portable Agent will be automatically configured to gather the data required to perform a subsequent IOC analysis; after the analysis is run, IOC hit results are available for further investigation.

In addition, Redline provides the ability to create an IOC Collector. This feature enables the collection of data types required for matching a set of IOCs.

WORKS WITH MIR

Combined with MIR, Redline is a powerful tool for accelerated live response. Here's a typical case:

- IDS or other system detects suspicious activity on a host
- From MIR, an investigator launches a remote live response script
- The MIR Agent running on the host captures and analyzes memory locally, streaming back a small XML audit that downloads in minutes rather than hours
- From MIR, the user can open the audit directly in Redline
- Using Redline, the investigator quickly identifies a malicious process, and writes an IOC describing the forensic attributes found in Redline
- Using MIR and MCIC, the investigator is quickly able to sweep for that IOC and discover all other systems on the network with the same (or similar) malware running

Have MIR Customers had Access to these IOCs Before?

These IOCs are new! However, much of the detection capability in this set of indicators has already been available to our MIR customers. The IOCs may look different though as a result of improvements in creation and testing. Mandiant started 2013 with a focus on taking better advantage of our threat intelligence. We plan to continue to improve the synthesis of our threat intelligence and our IOCs by improving our breadth, IOC creation process, IOC management process, and IOC testing. The majority of these indicators, or modified versions of them, will be integrated into the next IOC release.

What Is the FAMILY Designator in This Set of IOCs?

We are using a new IOC designator in these IOCs called "(FAMILY)." Mandiant's Threat Intelligence Unit tracks malware by common features seen in groups of binaries. We call those groupings of binaries "families." The IOCs included in this appendix are representatives of families of malware used by APT1. The new designator follows the family name in the "Name" field of the IOC, and the presence of (FAMILY) implies that that IOC applies to the whole family, not just one sample.

Why Do These IOCs Look Somewhat Different Than Other IOCs I Have Seen From Mandiant?

In many cases we have combined information that previously would have been in several indicators into a single indicator. Additionally, we have removed certain types of intelligence, since they are being released in separate appendices (such as FQDNs and IPs).

Additionally, some IOCs in this set are using file permutation blocks to catch variants of malware that might not be detected otherwise.

What Is a File Permutation block?

It is a different way to structure lists of File Item attributes to look for an entire family of malware versus only one or two pieces. For more information on this topic or most any other IOC questions go to https://forums.mandiant.com.

Will You Update These IOCs?

It is likely that we will make some changes to the IOCs in Appendix G as we get feedback. If updated, the updates will be available in the same location as the report http://www.mandiant.com/apt1.

Will You Be Releasing More IOCs Like This?

Currently, there are no plans for additional public releases of this magnitude.