NCCIC

National Cybersecurity and
Communications Integration Center

# Destructive Malware

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

March 2017

NCCIC

## SUMMARY

This white paper highlights a number of the destructive malware families analyzed by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and gives recommendations for victims on the best way to combat each specific family.  Destructive malware attacks are simple and fast to execute. In many cases, once the user knows that something odd is occurring on the system, it is already too late to do anything about it. Careful preparation and planning before an attack is the best mitigation against destructive malware.

# CONTENTS

# ACRONYMS

| | |
|---|---|
| APT | Advanced Persistent Threat |
| BE2 | BlackEnergy 2 |
| C2 | Command and Control |
| ICS-CERT | Industrial Control Systems Cyber Emergency Response Team |
| MBR | Master Boot Record |
| OS | Operating System |
| RAT | Remote Access Trojan |
| VBR | Volume Boot Record |

# DESTRUCTIVE MALWARE

## 1. OVERVIEW

Over the past decade, destructive malware has grown from a novel concept into an epidemic for both personal and commercial computing systems. Ransomware leads the pack with a growing popularity among attackers as a way to quickly extort money from victims, but file system and Master Boot Record (MBR) wiping have also gathered momentum as popular options for Advanced Persistent Threat (APT) groups to wreak havoc on the victim machine and to cover their tracks after an attack.

This white paper highlights a number of the destructive capabilities of malware families analyzed by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and gives recommendations for victims. Destructive malware attacks are simple to build and fast to execute. In many cases, once the user knows that something odd is occurring on the system, it is often already too late to do anything about it. Careful monitoring and backup policies are generally the most effective ways to mitigate the risk associated with destructive malware.

## 2. PURE WIPERS

These malware families are designed to destroy data or affect the ability of the target system to boot successfully. The action typically occurs either on receiving a command sent from the attacker or at a predetermined time.

### 2.1 Recommendation

Because of the likelihood that the system is actively being overwritten or encrypted, it is imperative to stop the process and any potential spreading of malware as quickly as possible. In these malware families, the chances of noticing that the wiper is running before it has completed are low. However, if the process is seen running across devices or is found on shared storage locations on the network, the victim may be able to disconnect all noncritical and known infected devices before further damage occurs. For most systems, it is recommended that the victim unplug the power from the system immediately and recover any essential data using another PC to mount the affected drive. If an infected system is evaluated to have a low business and operational impact, it is recommended that the victim disconnect the machine from the network to prevent the spread of malware before gathering logs and a memory capture to aid in forensic analysis.

### 2.2 Killdisk

Killdisk will erase the MBR of the victim system and delete files with any of 31 extensions. The malware takes an argument upon execution for a length of time until the destructive process is started. It then sets itself to run as a service and executes when the time requested by the attacker has elapsed or the attacker instructs the malware to execute immediately. The system is left in an unbootable state and must be rebuilt.

### 2.3 WhiteRose

This malware family is a derivative of Killdisk. Much of the code has been streamlined, along with targeting of new file extensions. As of the most recently discovered sample, 115 extensions are marked for destruction by the malware family. The malware has the ability to display a splash screen after the malware has finished executing as a “greeting” to the victim.

### 2.4 DarkSeoul

DarkSeoul wipes the MBR and Volume Boot Record (VBR) of the victim machine. The malware then proceeds to wipe blocks of data from the primary drive until the system crashes. Because of this logic condition, it is unknown what will be destroyed before the malware stops executing. Once critical Windows files are erased, an exception will cause the Operating System (OS) to crash.

### 2.5 DestFallen

DestFallen is a wiper that overwrites the MBR and some files before rebooting. The malware displays the text "Who Am I?" when the system reboots. Some advanced file recovery tools will likely be able to repair a number of lost files because DestFallen only overwrites the first 1K bytes of any file it targets.

### 2.6 Destover

Destover utilizes user credentials discovered by the attackers before deployment to attack network storage and other devices. Gathering a sample of the malware before sanitizing the device during recovery may be useful for determining compromised credentials.

## 3. MULTIFUNCTIONAL WIPERS

Multifunctional wipers are tools designed to perform multiple tasks for the attacker, including wiping of infected systems. These tools may be used in a wider array of malicious activity against the victim and should be analyzed for functionality as thoroughly as possible to determine the scope of the attacker's presence on the network. System logs, memory captures, and network indicators should be leveraged as much as possible to avoid losing track of what assets on the network have been either compromised or accessed by the attacker.

While it increases the likelihood that data may be lost by keeping the system powered on for the time needed to take a memory dump and collect logs, this information may be critical to gain insight to the attack before the device is powered down and removed from the network. If the data contained on the system is considered too valuable to risk losing, unplugging the system immediately may be necessary, but this could make tracking the threat considerably more difficult.

### 3.1 BlackEnergy 2 DSTR Plugin

A plugin for the BlackEnergy 2 (BE2) Remote Access Trojan (RAT), called DSTR, is capable of destroying both files on the file system as well as the system MBR. Because the DSTR plugin itself is executed by the BE2 RAT, it is most likely to be found after the RAT itself is located using antivirus utilities or Yara rules.

Careful preservation of data on the infected system is critical to knowing the scope of the infection. Multiple plugins for BE2 have been identified. Knowing which plugins were installed on a host can lead to new information about the attacker's motives and where the malware may have spread. Without this information, the victim may not know where to hunt for additional attacker presence on the network.

### 3.2 Shamoon/Disttrack

Shamoon/Disttrack attempts to spread to other devices on the local network. Command and Control (C2) communications are used to control the operation of the attack, but are not necessary if the threat actor has decided to designate a time for disk destruction beforehand.

Shamoon supports the ability to download and execute arbitrary executables, giving the attacker the ability to potentially spread the infection or download additional tools on the victim device for network traversal. In the event that the attacker did spread to other devices on the local network, preservation of the system logs and memory may allow for detection of other affected devices as well as other malware used by the attacker.

### 3.3 Gh0st RAT

Some Gh0st RAT variants include a feature that can wipe the MBR on the victim device and display a message to the user. In samples that have been analyzed by ICS-CERT, this message reads “Game Over!-Good Luck!” in red text, but this message may vary between samples.

The MBR can be repaired using a Windows recovery image, and no files on any other partitions are affected by the malware. The victim should disconnect from the network, repair the MBR of the compromised machine, take a capture of the system memory on startup, along with gathering a copy of the Gh0st malware, and file backups. The machine should be scanned by AV and triaged or rebuilt before being connected to the network again.

## 4. GENERAL RECOMMENDATIONS

The most important information for asset owners is that the scope of destructive malware is increasing at an alarming rate and preparation before an incident occurs is critical to avoid being caught off guard. In particular, creating frequent backups, validating that they can be used to restore a system, and then safeguarding those backups in an offline facility are the most reliable ways to recover from a destructive malware attack.

Asset owners should also be ready to pull network cables and power down systems that are found to be infected as promptly as possible to prevent the spread of destructive malware across the network, as well as mitigate damage from machines already infected. Maintaining up-to-date antivirus and timely operating system patches, along with rigorous network monitoring for suspicious traffic on all network connected environments, will greatly increase the operator’s ability to avoid general attacks.

For more detailed guidance on dealing with destructive malware, see the Additional Resources section.

# 5. ADDITIONAL RESOURCES

## 5.1 General Recommendations

https://ics-cert.us-cert.gov/tips/ICS-TIP-15-022-01—ICS-CERT recommendations on handling destructive malware.

https://www.justice.gov/criminal-ccips/file/872771/download—How to Protect Your Networks from Ransomware; interagency technical guidance document on protecting against ransomware attacks. Many of these recommendations are effective against all forms of destructive malware.

https://wired.com/wp-content/uploads/2016/03/RansomwareManual-1.pdf—Overview of what ransomware is and how to respond to an attack.

https://www.us-cert.gov/ncas/alerts/TA16-091A—Overview of what ransomware is and US-CERT recommendations on handling an attack.

## 5.2 Prevention of Ransomware Attacks

https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/whitepapers/top-recommendations-to-prevent-ransomware—Palo Alto recommendations on preparing for a ransomware attack.

https://www.symantec.com/connect/blogs/ransomware-dos-and-donts-protecting-critical-data—Best practices on preventing critical data loss due to ransomware.

https://zeltser.com/detect-impede-ransomware—Techniques and tools for detecting an attack that is in progress.

## 5.3 Recovery from Ransomware Attacks

http://www.thewindowsclub.com/list-ransomware-decryptor-tools—Collection of tools for decrypting files encrypted by select ransomware.

https://id-ransomware.malwarehunterteam.com/—Identification of ransomware based on the files it leaves on the drive after encryption.

https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml—List of known ransomware families and decryption tools for victims.

Department of Homeland Security

Office of Cybersecurity and Communications

National Cybersecurity and Communications Integration Center

NCCICCustomerService@hq.dhs.gov

1-888-282-0870

Industrial Control Systems Cyber Emergency Response Team

https://ics-cert.us-cert.gov