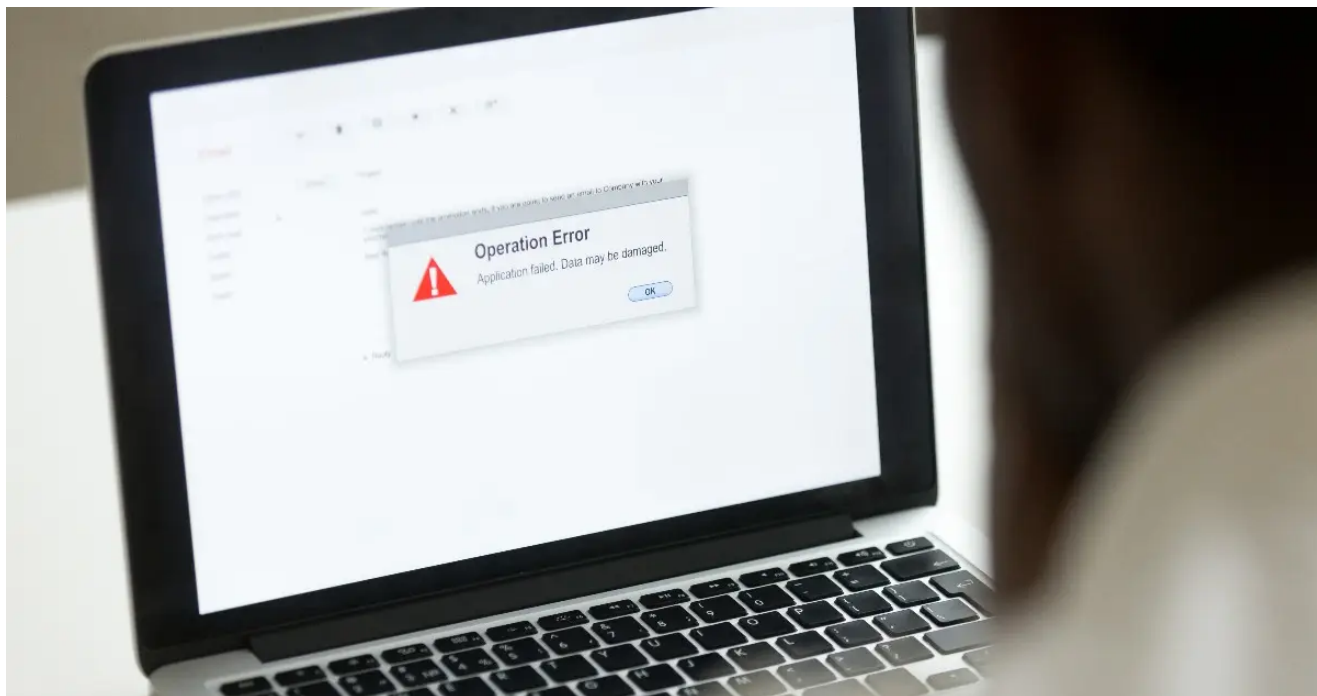


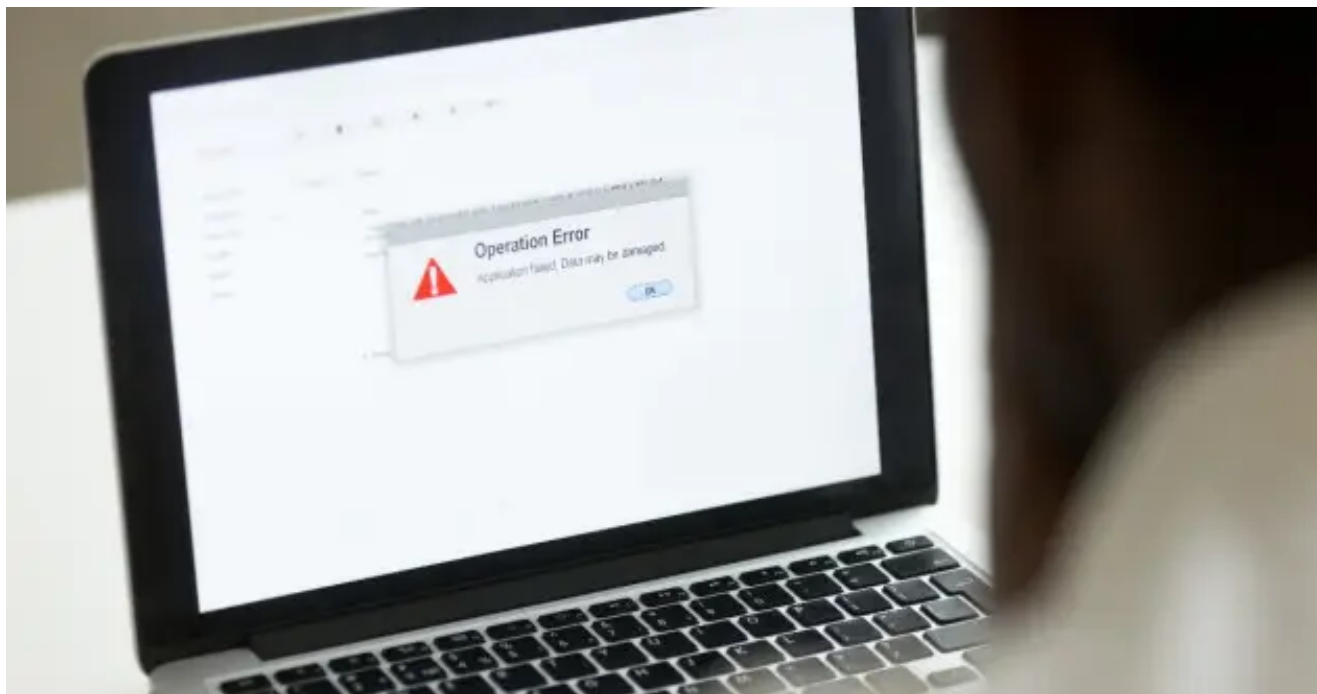
Third Wiper Malware Targeting Ukrainian Organizations

 securityintelligence.com/posts/caddywiper-malware-targeting-ukrainian-organizations/



[Home](#) [Malware](#)

CaddyWiper: Third Wiper Malware Targeting Ukrainian Organizations



[Malware](#) March 15, 2022

By [Christopher Del Fierro](#) co-authored by [John Dwyer](#) 3 min read

On March 1, 2022, ESET [reported](#) a third destructive data wiper variant used in attacks against Ukrainian organizations dubbed as CaddyWiper. CaddyWiper’s method of destruction is by overwriting file data with “NULL” values. This is the fourth sample of malware IBM Security X-Force has released public content for which has been reportedly targeted systems belonging to Ukrainian organizations ([IsaacWiper](#), [HermeticWiper/PartyTicket](#)). IBM Security X-Force obtained a sample of the CaddyWiper wiper and has provided the following technical analysis, indicators of compromise, and detections.

CaddyWiper Analysis

Upon execution, CaddyWiper first executes “*DsRoleGetPrimaryDomainInformation*” to determine the machine role of the system the wiper is running on. If the domain role is “*DsRole_RolePrimaryDomainController*,” CaddyWiper terminates and does not continue with any destructive functions. According to the [ESET](#), they observed CaddyWiper being deployed to target systems via a [Domain Controller](#) indicating the authors designed the wiper malware to be used in situations where the target’s Active Directory environment has been compromised.

```
result = DsRoleGetPrimaryDomainInformation(0, DsRolePrimaryDomainInfoBasic, &Buffer);
if ( Buffer->MachineRole != DsRole_RolePrimaryDomainController )// skip machine if Domain Controller
```

Figure 1: CaddyWiper system role check

If the target system is not a Domain Controller, CaddyWiper begins recursively wiping all data within “%SystemDrive%\Users” including hidden and operating system files. In the event a file is larger than 10 megabytes, the wiper only destroys the first 10 megabytes. If a file is currently locked by another process, CaddyWiper first attempts to take ownership of the file via “*SeTakeOwnershipPrivilege*” and then resumes wiping the file.

Name	Status	Description
SeRestorePrivilege	Disabled	Restore files and directories
SeSecurityPrivilege	Disabled	Manage auditing and security log
SeShutdownPrivilege	Disabled	Shut down the system
SeSystemEnvironmentPrivilege	Disabled	Modify firmware environment values
SeSystemProfilePrivilege	Disabled	Profile system performance
SeSystemtimePrivilege	Disabled	Change the system time
SeTakeOwnershipPrivilege	Enabled	Take ownership of files or other objects
SeTimeZonePrivilege	Disabled	Change the time zone
SeUndockPrivilege	Disabled	Remove computer from docking station

Figure 2: SeTakeOwnershipPrivilege attribute after running CaddyWiper on a locked file

Following “C:\Users”, CaddyWiper repeats the same process for all available drives from “D:” to “Z:”. When all the available drives have been wiped, CaddyWiper targets wipes disk partitions from “\\.\PHYSICALDRIVE9” to “\\.\PHYSICALDRIVE0” by overwriting the first

1920 bytes with NULL.

Detection

IBM Security X-Force has developed the following Yara signature to help identify instances of the CaddyWiper malware.

```
rule XFTI_CaddyWiper : CaddyWiper
{
meta:
author = "IBM Security X-Force"
description = "Detects CaddyWiper"
threat_type = "Malware"
rule_category = "Malware Family"
usage = "Hunting and Identification"
hash = "a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea"
yara_version = "4.0.2"
date_created = "15 March 22"
strings:
$s1 = "DsRoleGetPrimaryDomainInformation" ascii fullword
$hex1 = {
C645??43 //'C'
C645??3A //':'
C645??5C //'\'
C645??55 //'U'
C645??73 //'s'
C645??65 //'e'
C645??72 //'r'
C645??73 //'s'
}
$hex2 = {
C645??44 //'D'
C645??65 //'e'
C645??76 //'v'
C645??69 //'i'
C645??63 //'c'
C645??65 //'e'
C645??49 //'I'
C645??6F //'o'
C645??43 //'C'
C645??6F //'o'
C645??6E //'n'
C645??74 //'t'
C645??72 //'r'
C645??6F //'o'
C645??6C //'l'
}
```

```
condition:  
uint16(0) == 0x5A4D and all of them  
}
```

Indicators of Compromise

File System:

```
caddy.exe a294620543334a721a2ae8eaaaf9680a0786f4b9a216d75b55cfd28f39e9430ea
```

Recommendations

At this time, X-Force recommends organizations consider implementing the indicators listed in this report into their security operations. Additionally, global businesses should seek to establish sound insight into their respective networks, supply chains, third parties, and partnerships that are based in, or serve in-region institutions. It is also advised that organizations open lines of communications between relevant information sharing entities to ensure the receipt and exchange of actionable indicators.

If you have questions and want a deeper discussion about the malware and prevention techniques, you can schedule a briefing [here](#). Get the latest updates as more information develops on the [IBM Security X-Force Exchange](#) and the [IBM PSIRT blog](#).

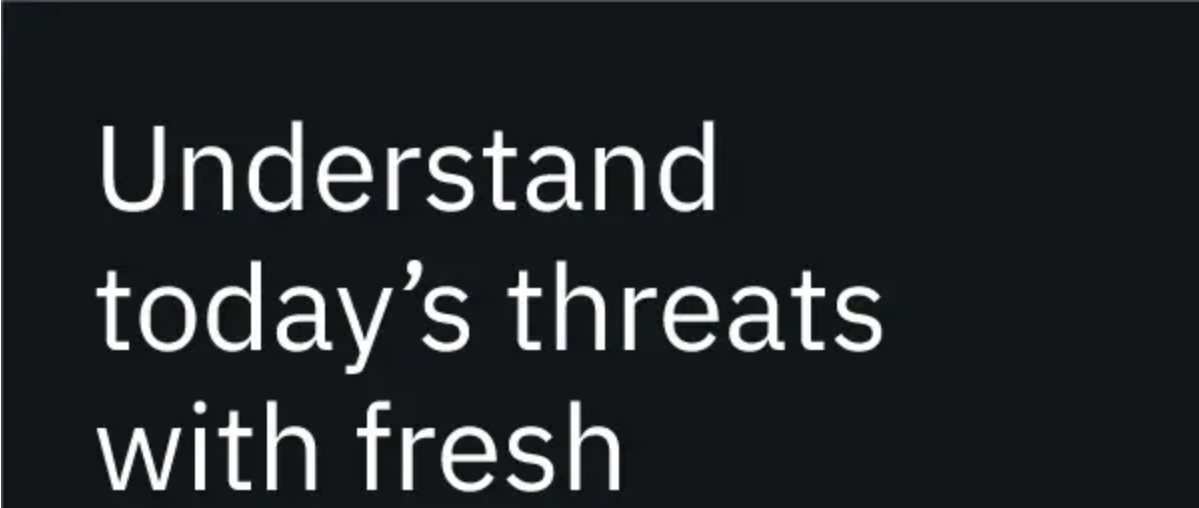
If you are experiencing cybersecurity issues or an incident, contact X-Force to help: US hotline 1-888-241-9812 | Global hotline (+001) 312-212-8034.

More cybersecurity threat resources can be found [here](#).

[Christopher Del Fierro](#)

X-Force IRIS Malware Reverse Engineer

Chris is a seasoned malware and threat researcher, certified system security engineer, MCP, and ethical hacker (CEHv5). Before joining IBM, Christopher was a...



Understand
today's threats
with fresh

intelligence

Get the report



IBM **Security**

