

New Wiper Malware Used Against Ukranian Organizations

 securityintelligence.com/posts/new-wiper-malware-used-against-ukranian-organizations/



Malware March 4, 2022

By John Dwyer co-authored by Kevin Henson 3 min read

March 7, 2022 Update

A correction has been applied to this blog, further analysis of the wiper malware revealed that the wiper leverages an implementation of the Mersenne Twister pseudorandom number generator (PRNG) and not ISAAC PRNG as originally reported. This blog has been updated to changing references from ISAAC PRNG to Mersenne Twister PRNG.

On February 24, 2022, [ESET reported](#) another destructive wiper detected at a Ukrainian government organization dubbed as IsaacWiper. This is the [third sample of malware](#) IBM Security X-Force has analyzed which has been reportedly targeting systems belonging to Ukrainian organizations. IBM Security X-Force obtained a sample of the IsaacWiper malware and has provided the following technical analysis, indicators of compromise and detections.

IsaacWiper Analysis

IsaacWiper is a destructive C++ malware that has been reported as being used in targeted campaigns against Ukraine organizations. The original filename of the analyzed sample is "Cleaner.dll" and contains a compile date of February 25, 2022, 15:48:07 UTC.

Upon execution, the function Start() is executed which begins by creating a log file within %ProgramData%. Following the creation of the log file, the wiper enumerates all physical drives on the target system by calling DeviceIoControl() with the control code IOCTL_STORAGE_GET_DEVICE_NUMBER. IsaacWiper checks the resulting physical drive list for devices with type 7 (FILE_DEVICE_DISK) to identify disk volumes and physical drives. With a list of disk objects, IsaacWiper leverages IOCTL_DISK_GET_DRIVE_GEOMETRY_EX and GetDiskFreeSpaceExW() to obtain the size and available free space of each disk.

Logfile %ProgramData%\log.txt generated by the IsaacWiper sample analyzed by IBM Security X-Force:

```
getting drives...
physical drives:
-- system physical drive 0: PhysicalDrive0
logical drives:
-- system logical drive: C:
-- logical drive: D:
start erasing system physical drive...
system physical drive -- FAILED
start erasing system logical drive C:
```

To begin the wiping activity, IsaacWiper leverages CreateFileW() and DeviceIoControl() with control code FSCTL_LOCK_VOLUME to lock the drive. With the drive locked, the wiper function first targets the PhysicalDrive by generating data created with a Mersenne Twister

pseudorandom number generator (PRNG) and overwriting the first 0x100000 bytes of the physical drive with the PRNG data.

After overwriting the PhysicalDrive, the malware starts overwriting drives and files. If the wiper can't open a file, the file is renamed to a temporary file containing "Tmf" and a random four-character string (example:Tmf3360.tmp) and overwritten with Mersenne Twister PRNG data.

If a volume can't be accessed, the wiper creates a hidden temporary directory and writes a file to it at the root of the volume (ex: %SystemDrive%\Tmd1234.tmp\Tmf5432.tmp). The temporary file Tmf5432.tmp is then filled with random data until the volume is out of space.

Mersenne Twister pseudorandom number generator (PRNG) data generation in the IsaacWiper sample analyzed by IBM Security X-Force.

```
v2 = v1;
v14 = 0;
MI[0] = GetTickCount();
for ( i = 1; i < 624; ++i )
    MI[i] = i + 0x0C078965 * (MI[i - 1] ^ (MI[i - 1] >> 18));
v4 = 624;
v14 = 624;
if ( !v2 )
    return a1;
result = a1;
if ( a1 <= 65536 )
{
    for ( j = &v2[a1 >> 2]; v2 < j; ++v2 )
    {
        if ( v4 == 624 )
        {
            twist(MT);
            v4 = v14;
        }
        v7 = MT[v4+1];
        v14 = v4;
        v8 = (((v7 >> 11) ^ v7) & 0xFF3A5BAD) << 7 ^ (v7 >> 11) ^ v7;
        *v2 = ((v8 & 0xFFFFDFBC) << 15) ^ v8 ^ (((v8 & 0xFFFFDFBC) << 15) ^ v8) >> 18;
    }
    v9 = a1 & j;
    v15 = v9;
    if ( (a1 & 3) != 0 )
    {
        if ( v4 == 624 )
        {
            twist(MT);
            v4 = v14;
            v9 = v15;
        }
        v10 = (MT[v4] >> 11) ^ MT[v4];
        v11 = (((v10 & 0xFF3A5BAD) << 7) ^ v10) & 0xFFFFDFBC << 15 ^ ((v10 & 0xFF3A5BAD) << 7) ^ v10;
        v15 = v11 ^ (v11 >> 18);
        sub_100087F0(v9, j, &v15, v9);
    }
    return a1;
}
return result;
}
```

Detection

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

```
import "pe"
rule XFTI_IsaacWiper : IsaacWiper
{
meta:
```

```
author = "IBM X-Force Threat Intelligence Malware Team"
description = "Detects the IsaacWiper destructive malware based the debug
messages and imports."
threat_type = "Malware"
rule_category = "Malware Family"
usage = "Hunting and Identification"
hash = "13037b749aa4b1eda538fda26d6ac41c8f7b1d02d83f47b0d187dd645154e033"
yara_version = "4.0.2"
date_created = "3 Mar 22"
date_updated = ""
reference = ""
strings:
$log_s6 = "getting drives" ascii wide nocase
$log_s7 = "start erasing physical drives" ascii wide nocase
$log_s8 = "start erasing logical drive" ascii wide nocase
$log_s9 = "start erasing system physical drive" ascii wide nocase
$log_s10 = "system physical drive" ascii wide nocase
$log_s11 = "start erasing system logical drive" ascii wide nocase
condition:
3 of ($log*) and (pe.dll_name == "Cleaner.dll" or
(pe.imports("kernel32.dll", "GetTickCount") and
pe.imports("kernel32.dll", "DeviceIoControl")))
}
```

Indicators of Compromise

File System:

```
Tmd<4 char>.tmp
```

```
Tmf<4 char>.tmp
```

```
%ProgramData%\log.txt
```

Notable Strings:

```
PhysicalDrive
```

```
\\.\\
```

```
*.*
```

```
C:\ProgramData\log.txt
```

```
getting drives...
```

```
physical drives:
```

```
-- system physical drive
```

```
-- physical drive
```

```
logical drives:
```

```
-- system logical drive:
```

```
-- logical drive:  
start erasing physical drives...  
-- FAILED  
physical drive  
-- start erasing logical drive  
start erasing system physical drive...  
system physical drive -- FAILED  
start erasing system logical drive  
Cleaner.dll  
[email protected]
```

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 communication 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](#).

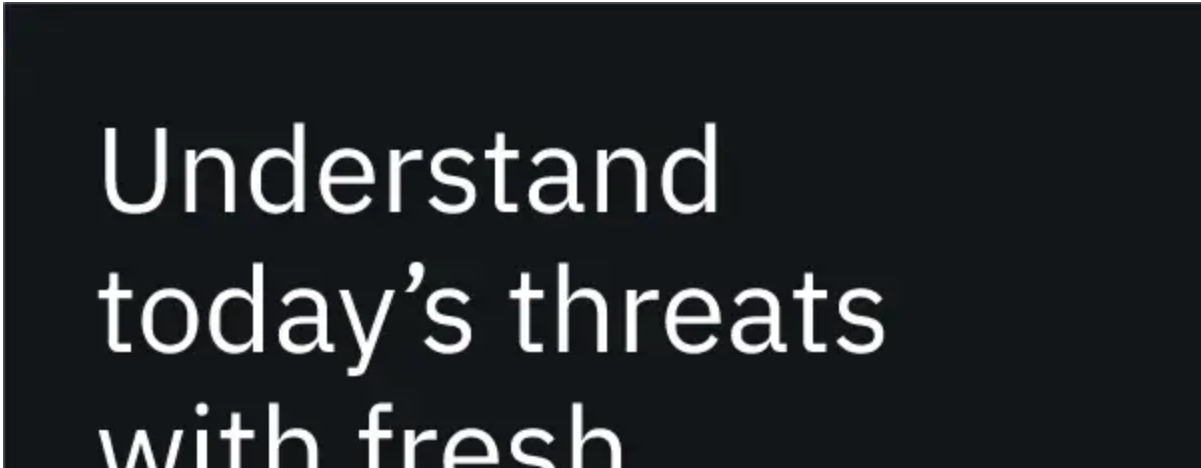
If you are experiencing cybersecurity issues or an incident, contact X-Force to help: US hotline 1-888-241-9812 | Global hotline (+001) 312-212-8034.

More cybersecurity threat resources are available [here](#).

[John Dwyer](#)

Global Threat Assessment Lead at IBM X-Force Incident Response

John (@TactiKoolSec on Twitter) is the Global Threat Assessment Lead for the IBM X-Force Incident Response team where he focuses on modeling adversary operat...



Understand
today's threats
with fresh

with fresh
intelligence

Get the report



IBM Security

