The Year of the Wiper

fortinet.com/blog/threat-research/the-year-of-the-wiper

January 24, 2023

FortiGuard Labs has been actively tracking wiper malware targeting Ukrainian organizations since the start of the 2022 Russia-Ukraine conflict. The sudden spike in wiper malware began early in the year with numerous new wiper samples targeted at Ukraine. It displayed a side of cyberattacks we rarely see: pure destruction. We published an article last April 2022 to help people understand the context, history, and technical setup of wiper attacks. This post focuses on what happened the rest of the year and how wiper malware and their attack scenarios have changed.

Affected Platforms: Multiple
Impacted Users: Large organizations
Impact: Data loss and OS and file corruption
Severity Level: High

Recap

Since that last report, quite a few new samples have been launched. Figure 1 shows an updated version of a timeline we have used in the past. In April, we were already surprised by the significant increase in wipers. As you can see, it increased even further over the rest of the year.

Figure 1 - Wiper malware timeline

Wipers in the War

Much of the wiper malware seen in the first half of 2022, whether attributed or not, was deployed against Ukrainian organizations. These include HermeticWiper, CaddyWiper, IsaacWiper, WhisperGate, and others. When you think about it, the growth in wiper malware during a conflict is hardly a surprise. It can scarcely be monetized. The only viable use case is destruction, sabotage, and cyberwar.

One interesting event was the AcidRain wiper malware that targeted the satellite modems of a global satellite communications provider, which caused modems to lose connections to their satellite network. The message was clear: even if a cyberattack is used to target Ukraine, its effects can easily spill over and affect other countries and organizations. It is vital that we track these new highly malicious attacks.

Motivation: Hacktivism

As the year progressed, pro-Russian hacktivism also increased. We saw that in our telemetry, showing, for example, an increase in DDOS attacks in Nordic countries, especially Finland (Figure 2).

Figure 2 - Fortinet combined IPS, malware, and botnet detections in the Nordic countries

However, hacktivism is usually associated with DoS and defacement attacks. But this time, some actors began repurposing their ransomware as wipers by not providing a decryption key. And if no decryption is provided, then ransomware essentially acts as a wiper. We saw actors begin to do this intentionally.

For instance, the Somnia ransomware was deployed at several Ukrainian organizations. The attackers compromised systems using a fake software installer and established a persistent presence. Like most ransomware attacks, they exfiltrated data and kept their access as long as needed. But at the end of the attack, no decryptor was offered, meaning the files remained encrypted and useless.

The Most Intriguing Wiper of the Year

The most intriguing wiper we documented in the second half of 2022 was one named ‘Azov.’ Its second version quickly drew media attention because it delivered a message written in the name of well-known security researchers. These researchers denied any connection to the malware. It also delivered a pro-Ukrainian message claiming it was using the malware to draw more attention to the Ukraine-Russia war. However, so far, no attribution has been made.

However, as it turned out, the message was not the most interesting part of the malware. It is also very compelling from a technical perspective.

First, it was written in the assembly language and built with the FASM tool. This is unusual because most new malware is written in languages such as python, .NET or C/C++. It also contradicts everyone’s first impression that it was a prank used to blame security researchers. However, it seems unlikely that anybody would go to the effort to write malware in assembly just for a joke.

It also implements polymorphic code creation to inject itself into legitimate EXE files on the infected machine. It then executes a backdooring function by injecting a modified version of itself into EXE files. This provides persistence to the malware because it can run again once the backdoored files are executed.

It also implements a variety of anti-analysis techniques:

- Opaque predicates
- Anti-debug
- Syntactic bloat and junk code
- Using CALL instructions instead of RET or JMP
- Dynamically creating the Import Address Table

All this demonstrates that this malware was not created for fun. It is a sophisticated wiper that implements a variety of modern techniques, clearly showing that a sophisticated threat actor.

Improving Performance

Ransomware authors understand that encryption speed is often crucial for a successful operation. Once encryption is started, they are in a race against the incident response team, who might detect them at any time. As a result, performance optimization was developed. Some new ransomware now implements a multi-threaded architecture that enables it to run multiple encryption threads in parallel. Other operators have realized that encrypting files in their entirety is time-consuming—and may not even be necessary. The BlackCat ransomware, for instance, implements multiple different encryption strategies with varying improvements in performance (see this VirusBulletin presentation).

A similar problem exists for wipers. Traditionally, wipers would erase an entire disk using a kernel driver, delete files using different techniques, and/or alter the content of files (more on techniques in our last article). These all take time. As a result, some authors began experimenting with performance optimization.

The DoubleZero wiper, for instance, only erases the first 4096 bytes of targeted files. This means that most of the data in an average file would not be erased. However, it’s also true that restoring these files at scale would be very impractical. For instance, modern Microsoft .docx files are essentially a collection of compressed XML files. Deleting the first 4096 bytes from them would corrupt the compression and the generic file structure, meaning these files would not work anymore. Recreating a functioning file with manual forensic work might be possible, but it is simply not feasible when dealing with hundreds or thousands of files.

The Azov wiper also implemented a somewhat more optimized wiping process. It does not remove all data in each file. Instead, it only targets 666 bytes in an alternating pattern (666 bytes overwritten, 666 bytes intact, 666 bytes overwritten, etc.) up to 4 GB.

Targeting OT

OT environments also saw their fair share of wipers. We already mentioned the attack against the satellite provider (and, by extension, the German windmills). Another interesting attack using the Industroyer.V2 malware targeted a Ukrainian high-voltage electric substation. That attack aimed to manipulate the electric relays to take the substation offline. In the context of OT, I would consider the use of the Industroyer.V2 malware in this context as a wiper. Traditional IT wipers have the goal of destroying the crown jewels of IT, the data. Industroyer.V2 was used to destroy the crown jewel of that substation, its operation.

If this was not enough, the Industroyer.V2 malware was deployed along with three other wipers, potentially from different actors:

- CaddyWiper for Windows machines
- AWFULSHRED for Linux, Unix machines
- SOLOSHRED for Solaris machines

This helps serve as a reminder that OT environments are being actively targeted by different threat actors, ranging from ransomware operators to state-sponsored APTs.

In Development

An interesting new project to pay attention to is the Endurance wiper. It is an open-source wiper that seemingly aspires to become ransomware. Figure 3 shows the malware’s features and readiness state as described by the author.

Figure 3 - Endurance wiper/ransomware features

Currently, Endurance’s file-wiping capabilities offer three wiping modes, with each mode defining how many times content should be overwritten. It also offers CONTENT deletion and FILE deletion functions. The CONTENT deletion (Figure 4) function is responsible for overwriting the contents of a file on disk.

Figure 4 - Loop to overwrite the file's content multiple times

The FILE deletion function (Figure 5) updates all file attributes and then erases the file from the disk.

Figure 5 - File deletion overwrites all file attributes and removes the file

This tool is actively in development, although at the time of testing, we had to fix the code build it. Since it is open-source, this could provide an easy entry point for attackers wanting to join the wiper/ransomware game.

Conclusion

2022 provided us with new perspectives on destructive malware. We saw different wiping techniques, different motivations, and differentmotivations, actors, and deployment scenarios. New wiper instances, such as the Azov and Endurance wipers, show that actors are actively engaged in increasingly malicious activity. They are also trying to address shorter threat detection and response time by effectively optimizing the performance of their wiping strategies. And we are also seeing increased attention being paid to OT networks, such as the example of the Industroyer.V2 malware. The point is clear. The gloves are off as threat actors increasingly engage in attacks designed with one purpose: to destroy their targets.

Fortinet Protection

The Fortinet Antivirus engine protects against all binaries discussed in this report using the following signatures:

W32/KillDisk.NCV!tr

W32/Agent.OJC!worm

W32/KillMBR.NHQ!tr

W32/CaddyWiper.NCX!tr

W32/KillFiles.NKU!tr.ransom

W32/KillMBR.NGI!tr

MSIL/Agent.FP!tr.dldr

MSIL/Agent.QWILJV!tr

W32/KillFiles.NKU!tr.ransom

MSIL/VVH!tr

MSIL/Agent.VVH!tr

W32/DISTTRACK.C!tr

W32/Generic.BQYIIWO!tr

W64/DistTrack.A!tr

W32/Ordinypt.5873!tr.ransom

W32/OlympicDestroyer.A!tr

W32/Petya.EOB!tr

W32/Petya.A!tr.ransom

W64/Petya.BG!tr

W32/Agent.F0FC!tr

W64/Dustman.KH!tr

W32/Distrack!tr

W32/Agent.XACVYS!tr

W32/Distrack!tr

MSIL/DZeroWiper.CK!tr

ELF/AcidRain.A!tr

MSIL/KillMBR.X!tr

MSIL/KillDisk.I!tr

W32/PossibleThreat

The FortiGuard Web Filtering service rates the C2 server as ‘Malicious’ and blocks it accordingly.

FortiMail and FortiSandbox detect and quarantine the malicious attachments in this campaign, and Fortinet's CDR (Content Disarm and Reconstruction) service can disable them.

FortiEDR natively detects and blocks the malicious executables identified in the report based on their behavior.

In addition to these protections, Fortinet can help train users to detect and understand phishing threats:

The FortiPhish Phishing Simulation Service uses real-world simulations to help organizations test user awareness and vigilance to phishing threats and to train and reinforce proper practices when users encounter targeted phishing attacks.

Our FREE NSE training program—NSE 1 – Information Security Awareness—includes a module on Internet threats designed to help end users learn how to identify and protect themselves from phishing attacks.

IOCs

650f0d694c0928d88aeeed649cf629fc8a7bec604563bca716b1688227e0cc7e - Azov

100c5e4d5b7e468f1f16b22c05b2ff1cfaa02eafa07447c7d83e2983e42647f0 - Somnia_07_08_22_with_FunnySomnia.rar

ac5e68c15f5094cc6efb8d25e1b2eb13d1b38b104f31e1c76ce472537d715e08 - Somnia_07_08_22_with_FunnySomnia.exe (Somnia)

99cf5c03dac82c1f4de25309a8a99dcabf964660301308a606cdb40c79d15317 - 1.exe (Cobalt Strike Beacon)

156965227cbeeb0e387cb83adb93ccb3225f598136a43f7f60974591c12fafcf - funnysomnia.exe

e449c28e658bafb7e32c89b07ddee36cadeddfc77f17dd1be801b134a6857aa9 - text.exe (Somnia*)

fbed7e92caefbd74437d0970921bfd7cb724c98c90efd9b6d0c2ac377751c9e5 - Ip_scanner.zip

06fe57cadb837a4e3b47589e95bb01aec1cfb7ce62fdba1f4323bb471591e1d2 - Ip_scanner.exe (Themida; Vidar)

1e0facd62d1958ccf79e049270061a9fce3223f7986c526f6f3a93ef85180a72 - Ip_scanner_unpacked.exe (Vidar)

3b2e708eaa4744c76a633391cf2c983f4a098b46436525619e5ea44e105355fe – DoubleZero

931b6b29e13d76a0e2e1e8b6910873d5ff7b88fd8c51cadf46057e47b695f187 – Endurance

BDF8B53D73CA1ED1B649B32A61608B2CF952397EF3D5FC2E6E9F41AD98C40110 – Cry Wiper

91a9180a9cf7674c34ed53a8aa4e36b798334d1f448aeaf1afb9add4fd322b6e – Fantasy

0ad0cd07ca69d8fd2b075fef6e6dd5e9f7debca92af3a6b84d83e51e23bc182d – Bruh Wiper

Learn more about Fortinet's FortiGuard Labs threat research and global intelligence organization and Fortinet's FortiGuard AI-powered Security Services portfolio. Sign up to receive our threat research blogs.