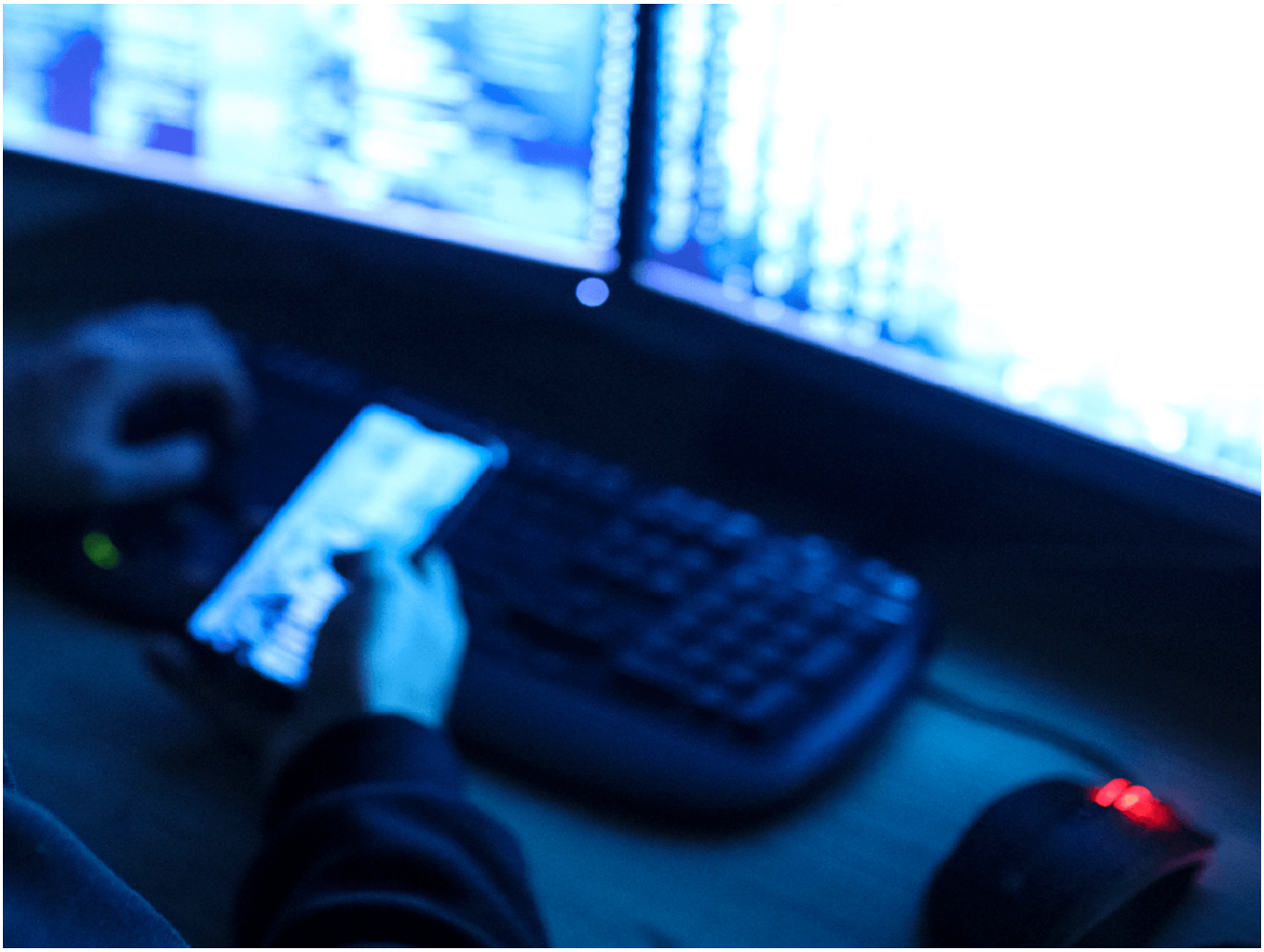
Wiper Malware Riding the 2021 Tokyo Olympic Games

fortinet.com/blog/threat-research/wiper-malware-riding-tokyo-olympic-games

July 26, 2021



FortiGuard Labs Threat Research Report

As society becomes increasingly reliant on technology, and as the world is more connected than ever, attacks by threat actors are not only more prevalent but also more disruptive. Because of the variety of agendas held by different malicious entities including—cybercriminals, hacktivists, nation states, etc.—attacks and disruptions targeted at high profile events are easy targets for sowing chaos, distributing malware, capturing or exfiltrating data, or even shutting down an event altogether. But regardless of the purpose, mass disruption and fear almost always occurs whether that was the intended goal of the attackers or not.

In that context, FortiGuard Labs has observed new threat samples targeting the 2021 Tokyo Olympic games. It includes a wiper component, which, if successful, could cause a disruption to targeted machines.

Background

The most recent attack targeting the Olympics was documented during the 2018 Winter Games. The lure was a malicious Word document titled, "*Russian figure skater won the PyeongChang Winter Olympics in South Korea.doc."* Once the user opened the document, the sample called and dropped a backdoor component, called Icefog. First discovered in 2013, the Icefog backdoor was used to attack sectors in the APAC region, with a focus on Japan and South Korea.

The threat actor group responsible for Icefog is very methodical. Targets are carefully chosen, and the group seems to know what they are after beforehand. Icefog leveraged CVE-2012-0158—a older vulnerability in Windows common controls—relying on the fact that many system administrators, especially those in organizations with a large number of computers (governments, NGOs, companies, various organizations, etc.), often find patching cumbersome. Because of this, older exploits such as this are often a successfully exploited vector, even though this particular vulnerability was over 6 years old at the time of the attack.

Fast forward to today, and in the wee hours of the Tokyo Olympic Games an interesting Wiper malware surfaced that reminded us of the same destructive malware that targeted the Pyeongchang Winter Games. This one is called “Olympic Destroyer.” Its file name is “【至急】東京オリンピック開催に伴うサイバー攻撃等発生に関する被害報告について.exe” (English translation: “(Urgent) Damage report in relation with cyber attacks targeting the Tokyo Olympics Games.exe”.

Although this particular malware is listed in some OSINT reports as potentially related to the Olympic Destroyer sample, we have not observed this to be the case. We also do not have any information on the delivery mechanism or methods used by the attacker, nor its intended targets. However, given its ties to the Olympics, and the relative short time frame for exploitation, we feel it is important that we share what we know so far about this new wiper malware.

***Note**: This is an evolving situation, and we will update this blog with relevant information when available.*

For a historical summary of attacks targeting the Olympic Games, please visit the Cyber Threat Alliance whitepaper, for which FortiGuard Labs was a contributing author:

UPDATING THE 2020 SUMMER OLYMPICS THREAT ASSESSMENT

Q. When was this malware found?

The malware was uploaded to a publicly available file repository on July 20th, 2021. A related file was subsequently found to have been uploaded to the same repository on July 17th, 2021. Both files have a PDF icon.

Q. Are Fortinet customers protected?

Yes, FortiGuard Labs has the following AV coverage in place for the malware:

W32/KillFiles.NKP!tr.ransom

All known IOCs are blocked by FortiEDR's advanced real-time protection and have already been added to our cloud intelligence to prevent further execution on customer systems.
All network IOC's are blocked by the WebFiltering client.

Q. How are the two files related?

Those files do not work in tangent with each other. The malware uploaded on July 20th has file deletion capability. The July 17th sample includes everything but the destruction feature.

Q. What does the malware do?

The destroyer malware searches for and deletes files with the following file extensions in the compromised machine.

.doc
.docm
.docx
.dot
.dotm
.dotx
.pdf
.csv
.xls
.xlsx
.xlsm
.ppt
.pptx
.pptm
.jtdc
.jttc
.jtd
.jtt
.txt
.exe
.log

The malware also silently accesses a benign adult site. Lastly, the threat deletes itself when all actions are completed.

Q. Does the malware have worm capability?

No, the malware does not have any propagation mechanism.

Q. Which organization did the malware target?

Currently, there is no information available pertaining to the targets or victims.

Q: Is there any similarity to Olympic Destroyer?

No, this malware and Olympic Destroyer do not have any similarity in code.

Q. Is there any nation state involvement?

At this time, there is insufficient evidence to support the involvement of any nation state. Based on the relative lack of sophistication of the code, however, it seems unlikely that a nation state is behind the malware.

Q: Is there anything note-worthy about the malware?

The malware has one interesting trick up its sleeve to deter researchers—it checks to see whether its own code has been modified. For example, the non-wiper (July 17th) sample includes the following code.

Essentially, what this means is that for certain functions, such as Enum_Procs, Check_Debuggers, and Check_VMX (seen in the above screenshot), the malware checks the first 5 bytes to see if it contains the “0xCC” opcode. This x86 assembly instruction stands for INT3, which tells debuggers to temporarily stop a running program. This method works as another anti-debug check because it detects to see if this function has been disabled.

The wiper (July 20th) version of this malware goes a step further. Aside from checking for “0xCC”, it also checks for others such as “0xEB” (call), “0xE8” (jmp), and “0xE9” (jmp). These instructions divert program flow away from the intended flow created by the original programmer. One reason to divert program flow is to hook and monitor Windows APIs. An API monitor can report what a program is doing while it is running, saving researchers a lot of reverse engineering time and effort. However, if any of this code has been modified to enable monitoring, the wiper exits without performing any malicious activities. This is yet another anti-analysis check to avoid behavioral monitoring. More information about diverting program flow can be found on the Microsoft Detours website.

As this is an ongoing event, FortiGuard Labs is monitoring the situation and will provide relevant updates for significant findings as they are uncovered.

MITRE Classifications

Defensive Evasion

- T1480: Execution Guardrails
- T1070.004: File Deletion
- T1027.002: Software Packing
- T1497: Virtualization/Sandbox Evasion
- T1497.001: System Checks
- T1497.003: Time Based Evasion

Discovery

- T1083: File and Directory Discovery
- T1057: Process Discovery
- T1518.001: Security Software Discovery
- T1497: Virtualization/Sandbox Evasion
- T1497.001: System Checks
- T1497.003: Time Based Evasion

Impact

T1485: Data Destruction

IOCs

Sample SHA-256:

fb80dab592c5b2a1dcaaf69981c6d4ee7dbf6c1f25247e2ab648d4d0dc115a97

c58940e47f74769b425de431fd74357c8de0cf9f979d82d37cdcf42fcaaeac32

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.

Learn more about Fortinet's free cybersecurity training, an initiative of Fortinet's Training Advancement Agenda (TAA), or about the Fortinet Network Security Expert program, Security Academy program, and Veterans program. Learn more about FortiGuard Labs global threat intelligence and research and the FortiGuard Security Subscriptions and Services portfolio.