Wiper malware targeting Japanese PCs discovered ahead of Tokyo Olympics opening

By Catalin Cimpanu

Published: 2022-12-13 · Archived: 2026-04-05 20:13:28 UTC

A Japanese security firm said it discovered an Olympics-themed malware sample that contains functionality to wipe files on infected systems and appears to be targeted at Japanese PCs.

The wiper's discovery, on Wednesday, came two days ahead of the opening ceremony for the 2021 Tokyo Olympics, scheduled to take place this Friday.

Discovered and analyzed by Japanese security firm Mitsui Bussan Secure Directions (MBSD), the wiper doesn't just delete all of a computer's data, and instead searchers only for certain file types located in the user's personal Windows folder, located at "**C:/Users/<username>/**".

Microsoft Office files are targeted for deletion, but also TXT, LOG, and CSV files, which can sometimes store logs, databases, or password information.

In addition, the wiper also targets files created with the Ichitaro Japanese word processor (emboldened below), which has led the MBSD team to believe that the wiper was specifically created to target computers in Japan—where the Ichitaro app is typically installed.

Targeted extensions:

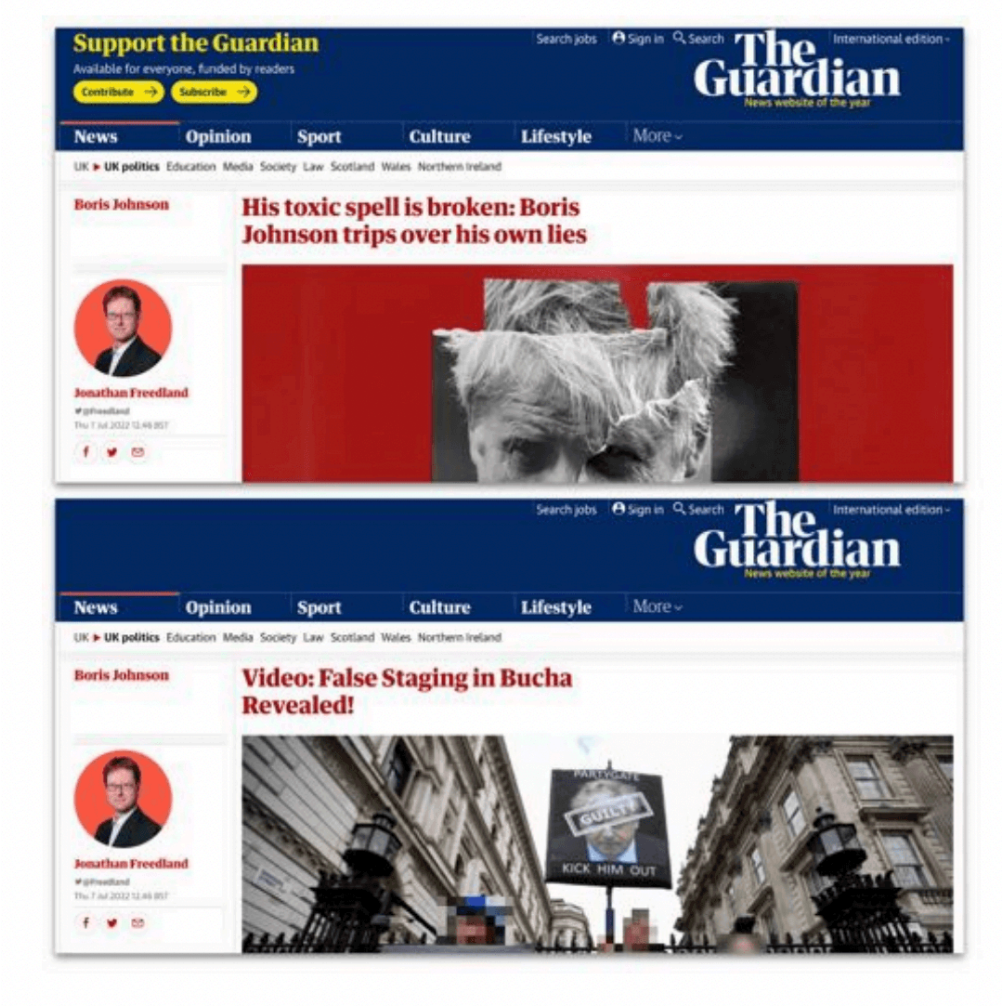
DOTM, DOTX, PDF, CSV, XLS, XLSX, XLSM, PPT, PPTX, PPTM, **JTDC, JTTC, JTD, JTT**, TXT, EXE, LOG

Figure 2: Defendant's Counterfeit Gucci Bedding

Other features found in the wiper also include a raft of anti-analysis and anti-VM detection techniques to prevent the malware from being easily analyzed and tested and the ability for the malware to delete itself once the wiping operation has finished.

Using adult traffic as a disguise

However, the most interesting feature is that the wiper also uses the cURL app to access pages on the XVideos adult video portal while the wiping behavior is taking place.



The MBSD team believes this behavior was added in an attempt to trick forensic investigators that the wiping behavior took place because the user got infected while accessing porn sites.

However, the MBSD team said the wiper was found in a Windows EXE file that was configured to look like a PDF file named: ***[Urgent] Damage report regarding the occurrence of cyber attacks, etc. associated with the Tokyo Olympics.exe***

"Since this malware is disguised using a PDF icon and only targets data under the Users folder, it is believed that the malware is intended to infect users who do not have administrator privileges," MBSD researchers Takashi Yoshikawa and Kei Sugawara wrote yesterday.

For now, only one copy of this malware sample was discovered, uploaded on VirusTotal on Tuesday, July 20. [*A second sample was discovered after this article went live.*]

FBI warns about possible cyberattacks aimed at the Olympics

The wiper's discovery came a day after the US Federal Bureau of Investigation had sent out a private industry alert [PDF] to US companies about the possibility that threat actors might target the Tokyo Olympics this year.

Cyberattacks carried out by Russia's military hacking groups have taken place during the last two Olympic Games.

After Russian athletes were banned from participating at the Rio 2016 Summer Olympics under the Russian flags in light of a state-sponsored doping scandal, the APT28 (Fancy Bear) group breached the World Anti-Doping Agency (WADA) in August 2016 and later leaked files online.

After the ban was extended for the PyeongChang 2018 Winter Olympics, Russian hackers deployed the Olympic Destroyer wiper during the games' opening ceremony in an attempt to cripple the organizers' internal network.

The ban on Russian athletes competing under the Russian flag is still in place for the Tokyo Olympics.

No previous article

No new articles

Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.
