Circular 211 – "UltiEr.exe" Malware Possessed by Almost Certainly Iranian Cyber Actors

TRAFFIC LIGHT PROTOCOL (TLP): AMBER – RECIPIENTS MAY ONLY SHARE **TLP: AMBER** INFORMATION WITH MEMBERS OF THEIR OWN ORGANIZATION, AND WITH ESTABLISHED CLIENTS, CUSTOMERS, CYBERSECURITY PROVIDERS, OR VENDORS WHO NEED TO KNOW THE INFORMATION TO PROTECT THEMSELVES OR PREVENT FURTHER HARM. THIS INFORMATION IS MADE AVAILABLE FOR CYBERSECURITY PURPOSES ONLY. THIS INFORMATION IS NOT AUTHORIZED FOR DISSEMINATION OR RELEASE, DIRECTLY OR INDIRECTLY, TO ANY FOREIGN GOVERNMENT.

Circulars are intended to inform cybersecurity specialists of cyber actors' tactics, techniques, and procedures along with associated indicators when available, to assist in network defense capabilities and planning.

Details

In late February 2026, almost certainly Iranian cyber actors possessed the "UltiEr.exe" malware.

The "UltiEr.exe" malware is a wiper (T1561) targeting Windows operating system (OS). It first attempts to overwrite the master boot record (MBR) of PhysicalDrive1 and PhysicalDrive0 by writing the repeating hex string "0x55aa" to the first 512 bytes of each drive. "0x55aa" is a valid boot signature, so the BIOS will recognize this MBR as valid and try to boot the drive, but will not be able to, as the bootloader and the partition table have been overwritten.

"UltiEr.exe" then uses "IOCTL_DISK_DELETE_DRIVE_LAYOUT" on the C: drive to remove the boot signature from the MBR, which immediately crashes the OS if it is running on the C: drive. No network activity was observed from "UltiEr.exe" when running. "UltiEr.exe" requires admin privileges to access the physical drives. If the wiper is run without admin privileges, it will terminate without modifying the system.

The "UltiEr.exe" malware appears to be a simple wiper. It will render a drive unable to successfully boot, but the contents of the drive are not modified and are recoverable. Iranian cyber actors have used wipers in the past as either cyber network attacks or as ransomware.

The "UltiEr.exe" malware has the following characteristic:

MD5	1772cf96e2a04d656c6e6c16fe2775e7
SHA-1	376bd010b2047b2628ecdf160f5db9a8a410b190
SHA-256	18b8aca096026afb56f74a14ee8567c8221c37f355c4dcda8ceac75f65807e14

Detection and Mitigation Techniques

The following is a YARA rule[1] for this malware:

```
rule geometry_delete_wiper
{
meta:
date = "2026-03-09"
classification = "UNCLASSIFIED//FOR OFFICIAL USE ONLY"
strings:
$IOCTL1 = { BA 00 00 07 00 }
$IOCTL2 = { BA 00 C1 07 00 }

$L1 = { 41 B8 55 00 00 00 0F 1F 40 00 F6 C1 01 B8 AA FF FF FF 41 0F 44 C0 88 02 FF C1 48 8D 52
01 48 63 C1 48 3B C6 72 E4 }
$L2 = { 83 F1 67 B8 81 80 80 80 F7 E9 03 D1 C1 FA 07 8B C2 C1 E8 1F 03 D0 69 C2 FF 00 00 00
2B C8 }
condition:
all of ($IOCTL*) and 1 of ($L*)
```

For additional information on Iranian cyber threats, see CISA's Iran Threat Overview and Advisories. CISA offers a Known Exploited Vulnerabilities Catalog and use of free CISA Cyber Hygiene Vulnerability Scanning that evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. In addition, ensuring software vendors maintain high standards of security and transparency can reduce the risk of compromise and preempt cyberattacks, given that cyber incidents at a firm may result from insecurity of the vendor's product or a compromise of a firm's vendor itself.

[1] YARA is a tool for identifying malicious files by defining and matching patterns among malware families. See: Department of Homeland Security National Cybersecurity and Communications Integration Center. *Using YARA for Malware Detection*. 2015. https://www.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_YARA_S508C.pdf

Reporting Suspicious Activity

To report an intrusion and request technical assistance, contact CISA at central@cisa.dhs.gov or 888-282-0870, or FBI through a local field office or FBI's Cyber Division at CyWatch@fbi.gov or 855-292-3937, or any of the U.S. Secret Service's local field offices to report a crime.

We would like to hear from you on the usefulness of these reports to continuously improve them. Please take a moment to let us know what works and how we can better meet your needs. We invite all input but are particularly interested in input on the following:

- The usefulness of the reports
- The appropriate level of detail
- Ideas for improving the relevance of the reports
- Steps to make information more salient
- Ways to provide more appropriate context
- Topics for future reports

Please direct comments or questions to OCCIP-Coord@treasury.gov.