Cyber threat activity in Ukraine: analysis and resources

msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/

UPDATE 27 Apr 2022: See ***Updated malware details and Microsoft security product detections*** below as discussed in the **Special Report: Ukraine**.

UPDATE 02 MAR 2022: See ***Updated malware details and Microsoft security product detections*** below for additional insights and protections specific to the evolving threats we have identified impacting organizations with ties to Ukraine.

Microsoft has been monitoring escalating cyber activity in Ukraine and has published analysis on observed activity in order to give organizations the latest intelligence to guide investigations into potential attacks and information to implement proactive protections against future attempts.

We've brought together all our analysis and guidance for customers who may be impacted by events in Ukraine into this single location for ease of consumption, all of which is linked below. In this blog, we've also included general security guidance for organizations to build cyber resilience. As the situation in the region develops, we will continue to publish new insights and add to this set of resources.

Microsoft has been notifying customers in Ukraine of activity, where possible, and closely coordinating with the government in Ukraine. This support is ongoing.

We have also summarized information about what we are doing around protecting organizations in Ukraine from cyberattacks; protecting against state-sponsored disinformation campaigns; supporting humanitarian assistance; and protecting our employees: Digital technology and the war in Ukraine.

Published Microsoft analysis of malicious activity in Ukraine

Phishing attacks on Ukrainian soldiers:

> February 25, 2022 | RiskIQ: UNC1151/GhostWriter Phishing Attacks Target Ukrainian Soldiers

Recent disk wiping attacks:

> February 24, 2022 | RiskIQ: HermeticWiper Compromised Server Used in Attack Chain

Advanced threat actor ACTINIUM which has consistently pursued access to organizations in Ukraine or entities related to Ukraine affairs:

- February 4, 2022 | Microsoft Security Blog: ACTINIUM targets Ukrainian organizations
- February 4, 2022 | RiskIQ threat intelligence article: ACTINIUM targets Ukrainian organizations
- February 4, 2022 | Microsoft Threat Analytics article (requires a license): Threat Insights: ACTINIUM targets Ukrainian organizations

Destructive malware operation and malware family known as WhisperGate targeting multiple organizations in Ukraine:

- January 15, 2022 | Microsoft on the Issues Blog: Malware attacks targeting Ukraine government
- January 15, 2022 | Microsoft Security Blog: Destructive malware targeting Ukrainian organizations
- January 15, 2022 | RiskIQ threat intelligence article: Destructive malware targeting Ukrainian organizations

OSINT (open source intelligence) articles around activity in Ukraine are published regularly into the RiskIQ Community. The full list is available here: RiskIQ Community articles on Ukraine activity.

Security guidelines and recommendations

We recommend that customers review their security posture and implement best practices to build resilience against today's threats. Below are recommendations and links to resources:

1. **Cybersecurity hygiene:** Organizations should harden all systems by following basic principles of cyber hygiene to proactively protect against potential threats. Microsoft recommends taking the following steps:
    - Enable multifactor authentication
    - Apply least privilege access and secure the most sensitive and privileged credentials
    - Review all authentication activity for remote access infrastructure
    - Secure and manage systems with up-to-date patching
    - Use anti-malware and workload protection tools
    - Isolate legacy systems
    - Enable logging of key functions
    - Validate your backups
    - Verify your cyber incident response plans are up to date
2. **Microsoft Security Best Practices:** Microsoft customers can follow best practices that provide clear actionable guidance for security related decisions. These are designed to improve your security posture and reduce risk whether your environment is cloud-only, or a hybrid enterprise spanning cloud(s) and on-premises data centers: Microsoft Security Best Practices

3. **Protect against ransomware and extortion:** Human-operated ransomware attacks can be catastrophic to business operations and are difficult to clean up, requiring complete adversary eviction to protect against future attacks. Follow our ransomware specific technical guidance to help prepare for an attack, limit the scope of damage, and remove additional risks: Human-operated ransomware

Updated malware details and Microsoft security product detections

For customers utilizing Microsoft security products, we continue to build and release protections for the evolving threats we have identified impacting organizations with ties to Ukraine. As noted in the published analysis above, there are multiple actors using a variety of tools and techniques in this dynamic threat landscape. Some of these threats are assessed to be more closely tied to nation-state interests, while others seem to be more opportunistically attempting to take advantage of events surrounding the conflict. We have observed attacks reusing components of known malware that are frequently covered by existing detections, while others have used customized malware for which Microsoft has built new comprehensive protections.

Destructive wiper attacks

Beginning with WhisperGate, Microsoft continues to observe destructive malware attacks impacting organizations in Ukraine. These attacks are often the final stage to intrusions that, in some cases, may have predated the current military actions in Ukraine. We assess that the intended objective of these attacks is the disruption, degradation, and destruction of targeted resources. The Microsoft Threat Intelligence Center (MSTIC) assesses that organizations within Ukraine continue to be at high-risk for destructive operations for the foreseeable future.

Microsoft Defender Antivirus provides detections for the wiper attacks in build version **1.363.797.0** or newer. Customers utilizing automatic updates do not need to take additional action. Enterprise customers managing updates should select the detection build **1.363.797.0** or newer and deploy it across their environments.

The following is a list of high-level activities and the related malware that Microsoft has identified and is protecting customers against:

WhisperGate

Limited-scope destructive malware attack on January 13, 2022 impacting dozens of systems spanning multiple government, non-profit, and information technology organizations, all based in Ukraine. MSTIC tracks the actor responsible for this attack as DEV-0586 and has not linked it to a previously known activity group. We assess that DEV-0586 continues to be active in Ukraine but is also targeting other countries within the region.

FoxBlade and SonicVote

Destructive malware attack originally discovered on February 23, 2022 impacting hundreds of systems spanning multiple government, information technology, financial sector, and energy organizations predominately located in or with nexus to Ukraine. MSTIC has attributed events associated with FoxBlade with medium confidence to IRIDIUM (previously tracked as DEV-0665). Microsoft assesses there will be a continued risk for destructive activity from this group, as we have observed follow-on intrusions since February 23 involving these malicious capabilities. Microsoft is tracking the following malware families related to this activity:

- FoxBlade (aka HermeticWiper / HermeticWizard)
- SonicVote (aka HermeticRansom)

IRIDIUM has also periodically leveraged a renamed version of the SysInternals utility *sdelete* (renamed by IRIDIUM to *cdel.exe*) to perform targeted secure deletion of areas of the file system using the following command-line pattern:

```
c:\Windows\System32\cmd.exe /C C:\Windows\cdel.exe -accepteula -r -s -q c:\Users & C:\Windows\cdel.exe -accepteula -r -s -q c:\ProgramData
```

Lasainraw (aka IsaacWiper)

Limited destructive malware attack originally identified by ESET on February 25, 2022. Microsoft continues to investigate this incident and has not currently linked it to attributed threat actors.

DesertBlade

Limited destructive malware attack in early March 2022 impacting a single Ukrainian entity. Similar to other destructive capabilities, DesertBlade, which is implemented in Golang, was deployed via hijacked Group Policy Objects (GPOs). DesertBlade is responsible for iteratively overwriting and then deleting overwritten files on all accessible drives (sparing the system if it is a domain controller). Due to the nature of the investigation and partnerships involved, Microsoft is currently not able to share samples of DesertBlade. However, we can share the following hashes as examples of the DesertBlade family:

- a71c8306b6b8a89c18dea3b1490037593737d59b023000f24da94e3275600b59
- 4ca63406ff189301ccbb54daa6e2da4bc5d03ffc1a8a9756717d95d26abc3906

The following Yara rule can be used to detect DesertBlade using these hashes:

```
rule DesertBlade
{
    meta:
```

```
        author = "Microsoft Threat Intelligence Center (MSTIC)"
        description = "Detects Golang package, function, and source file
names observed in DesertBlade samples"
        hash =
"a71c8306b6b8a89c18dea3b1490037593737d59b023000f24da94e3275600b59"
    strings:
        $s1 = "main.wipe\x00\x00"
        $s2 = "main.getRandomByte\x00\x00"
        $s3 = "main.drives\x00\x00"
        $s4 = "main.main.func3\x00\x00"
        $s5 = "walk.volumeNameLen\x00\x00"
        $s6 = "windows.GetLogicalDriveStrings\x00\x00"
        $s7 = "api.ExplicitAccess\x00\x00"
        $s8 = "go-acl.GrantSid\x00\x00"
        $s9 = "/src/w/w.go\x00\x00"
    condition:
        uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and
        filesize < 5MB and filesize > 1MB and
        all of ($s*)
}
```

FiberLake (aka DoubleZero)

On March 22, 2022 CERT-UA published details on a .NET capability being used in destructive attacks tracked by Microsoft as FiberLake (aka DoubleZero). Microsoft has observed FiberLake being used in attacks targeting Ukraine broadcast/media organizations. Microsoft is continuing to investigate this incident and has not currently linked it to known threat activity.

CaddyWiper and AprilAxe (aka ARGUEPATCH)

CaddyWiper was first discovered by ESET on March 14, 2022 and has been observed by Microsoft impacting a limited number of organizations in targeted attacks. CaddyWiper is a destructive capability that results in file and drive overwriting, rendering compromised systems unbootable. On April 1, 2022, Microsoft identified a new variant that involved a multi-stage loading process.

In this new variant, the threat actor leveraged a backdoored IDA debugger server executable, which Microsoft has named AprilAxe. AprilAxe is designed to de-obfuscate and load malicious code from disk. In all observed intrusions, the loader is paired with a variant of CaddyWiper. Microsoft has observed multiple impacted organizations across government, natural resources, banking, and energy organizations. ESET published technical details on this new version of CaddyWiper/ARGUEPATCH. In line with ESET, MSTIC also attributes the intrusion activity and capabilities to IRIDIUM.

Industroyer.B (aka Industroyer2)

On April 8, 2022, Microsoft observed AprilAxe and CaddyWiper being staged to target an energy organization in Ukraine. During this intrusion, the actors also deployed a malicious ICS/SCADA utility named Industroyer 2, which is capable of interacting with industrial control systems. CERT-UA and ESET published additional technical details on this capability. In line with ESET, MSTIC attributes this intrusion activity and capability to IRIDIUM.

Related protections

Customers are encouraged to turn on cloud-delivered protection and automatic sample submission in Microsoft Defender Antivirus. These capabilities use artificial intelligence and machine learning to quickly identify and stop new and unknown threats. As we continue to investigate these attacks and uncover new data, we will add or update protections.

Microsoft Defender Antivirus and Microsoft Defender for Endpoint customers should look for the following family names for activity related to the wiper attacks:

- WhisperGate
- FoxBlade
- Lasainraw
- SonicVote
- CaddyWiper
- AprilAxe
- FiberLake
- Industroyer
- DesertBlade

The observed wiper attacks can be further limited through additional hardening configurations. When enabled, these features bring more resilience to customer defenses in addition to defending against these specific wiper attacks:

- Tamper protection prevents common techniques observed to disable security protections on endpoints.
- Controlled folder access allows only trusted apps to access protected folders. It is typically effective at blocking these wiper attacks.

Unattributed threat activity

As part of continued efforts by the MSTIC and Microsoft 365 Defender Research teams to identify threat activity and protect organizations, we continue to discover unattributed threat activity. We will continue to analyze activity and build detections for these threats as they are identified.

As with any observed nation-state actor activity, where possible, Microsoft directly and proactively notifies customers that have been targeted or compromised, providing them with information they need to help guide their investigations. MSTIC is also actively working with members of the global security community and other strategic partners to share information that can help address this evolving threat through multiple channels. Microsoft uses DEV-#### designations as a temporary name given to an unknown, emerging, or a developing cluster of threat activity, allowing MSTIC to track it as a unique set of information until we reach a high confidence about the origin or identity of the actor behind the activity.

Common secondary intrusion behaviors

Many of the observed attacks have made use of known malware and intrusion tactics, techniques, and procedures (TTPs) that are detected by Microsoft Defender for Endpoint using these common alerts:

- Suspicious remote activity
- Suspicious access to LSASS service
- Microsoft Defender Antivirus tampering
- Suspicious remote activity

Customers who see incidents that tie one or more of these indicators together should prioritize investigation of the affected devices.

Opportunistic phishing campaigns

Taking advantage of interest in the geopolitical conflict, attackers have been observed using tailored domains in phishing attacks. Microsoft SmartScreen and the network protection feature in Microsoft Defender for Endpoint provide protections for customers lured to these domains, including, but not limited to, the following:

- help-for-ukraine[.]eu
- tokenukraine[.]com
- ukrainesolidarity[.]org
- ukraine-solidarity[.]com
- saveukraine[.]today
- supportukraine[.]today

Hunting for related attacks

Microsoft Sentinel and Microsoft Defender for Endpoint customers can hunt for related activity through the queries below:

Microsoft Sentinel

Microsoft Sentinel offers detection and threat hunting analytics for techniques observed in relation to these threats. These analytics can be found in the Microsoft Sentinel portal or via the Microsoft Sentinel GitHub.

Crash dump disabled on host

This query looks for registry keys being set on a host in order to prevent crash dumps being created.

https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/SecurityEvent/Crashdumpdisabledonhost.yaml

New EXE deployed via Default Domain or Default Domain Controller Policies

This query looks for executables executed on host that appear to have been deployed via the Default Domain Policy or the Default Domain Controller Policy. These policies are not typically used for distributing executables.

https://github.com/Azure/Azure-Sentinel/blob/master/Detections/SecurityEvent/NewEXEdeployedviaDefaultDomainorDefaultDomainControllerPolicies.yaml

Potential renamed Sdelete usage

This query looks for command line parameters associated with recursive use of Sdelete against the C drive where the originating process isn't named *sdelete.exe.*

https://github.com/Azure/Azure-Sentinel/blob/master/Detections/SecurityEvent/Potentialre-namedsdeleteusage.yaml

Sdelete deployed via GPO

This query looks for Sdelete being deployed via GPO and run recursively on a host.

https://github.com/Azure/Azure-Sentinel/blob/master/Detections/SecurityEvent/SdeletedeployedviaGPOandrunrecursively.yaml

Microsoft Defender for Endpoint

To locate possible exploitation activity, run the following queries:

Surface suspicious MSHTA process execution

Use this query to look for MSHTA launching with command lines referencing DLLs in the AppData\Roaming path.

```
DeviceProcessEvents
| where FileName =~ "mshta.exe"
| where ProcessCommandLine has_all (".dll", "Roaming")
| where ProcessCommandLine contains @"Roaming\j"
| extend DLLName = extract(@"[jJ][a-z]{1,12}\.dll", 0, ProcessCommandLine)
```

Surface suspicious Scheduled Task activity

Use this query to look for Scheduled Tasks that may relate to actor activity.

```
DeviceProcessEvents
| where ProcessCommandLine has_all ("schtasks.exe", "create", "wscript",
"e:vbscript", ".wav")
```

Potential renamed *sdelete* usage

Use this query to look for command line parameters associated with the use of a renamed Sysinternals sdelete tool to delete multiple files on the C drive as part of destructive attacks on a host.

```
DeviceProcessEvents
| where InitiatingProcessFileName !~ "sdelete.exe"
and InitiatingProcessCommandLine has_all ("-accepteula", "-r", "-s", "-q", "c:/")
and InitiatingProcessCommandLine !has ("sdelete")
```

Microsoft continues to investigate these attacks and improve protections as new data is analyzed. In addition, Microsoft Sentinel and Microsoft 365 Defender have a range of existing queries for the detection of common techniques, such as lateral movement and privilege escalation. We recommend customers use these queries to identify common attacker techniques being used in these attacks.

We continue to monitor activity and will update this page with more information as the situation develops.