Summary of Russian Disruptive and Destructive Cyber Attacks, Ukraine 2022 and Prior

Cyber Espionage (CE) | Critical Infrastructure (CI)
Fusion (FS) | Hacktivism (HK)
Strategic (ST)

May 4, 2022 08:22:09 PM, 22-00004460, Version: 11.0

Executive Summary

- Mandiant has observed several significant disruptive and destructive attacks related to the 2022 Ukraine conflict to date.
- We expect to see additional disruptive and destructive attacks against Ukrainian targets, particularly in the government, financial, energy and utilities, and media and entertainment sectors, and potentially international organizations as well.
- There is significant precedent for Russian use of disruptive and destructive cyber attacks, particularly to support political and military objectives in Ukraine, including sabotage, compellence, punishment, and undermining public confidence in the Ukrainian government and institutions.

Threat Detail

New Version Details

Version 11, May 4, 2022: Clarified details of previously reported incidents.
Version 10, April 13, 2022: Added newly reported incidents.
Version 9, April 6, 2022: Incorporated additional details for relevant incidents.
Version 8, March 29, 2022: Added a newly reported incident.
Version 7, March 22, 2022: Added a newly reported incident.
Version 6, March 21, 2022: Updated to reflect APT28 attribution for NEARTWIST.
Version 5, March 18, 2022: Included additional relevant threat activity.
Version 4, March 15, 2022: Added links, industry tags.
Version 3, March 14, 2022: Added reports of other potentially relevant incidents.
Version 2, March 4, 2022: Minor changes including updating malware names and adding alternative names.

2022 Ukraine Crisis

Russia began amassing troops along its border with Ukraine in fall 2021, prompting warnings and disclosures from U.S. and European officials. Mandiant identified multiple examples of cyber espionage, cyber attack, and information operations activity ahead of Russia's Feb. 24, 2022 invasion of Ukraine (22-00000226, 22-00003826, 21-00025520).

We have observed several significant disruptive and destructive cyber attacks targeting Ukraine to date, summarized in Table 1 below. While we currently lack sufficient technical evidence to provide further insight into attribution for these incidents, it is highly likely that they are a continuation of Russian-sponsored campaigns affecting Ukrainian systems in the past few months. We expect to see Russian cyber threat actors conduct additional disruptive and destructive attacks against Ukrainian targets.

We also anticipate that Russia could task its offensive cyber capabilities to conduct retaliatory actions, particularly against the government, financial services, and energy and utilities sectors. Organizations making public statements condemning Russian aggression and/or supporting Ukraine—particularly those taking actions to restrict Russian participation in international commerce, competitions, and events—face elevated risks of future reprisal (22-00004449).

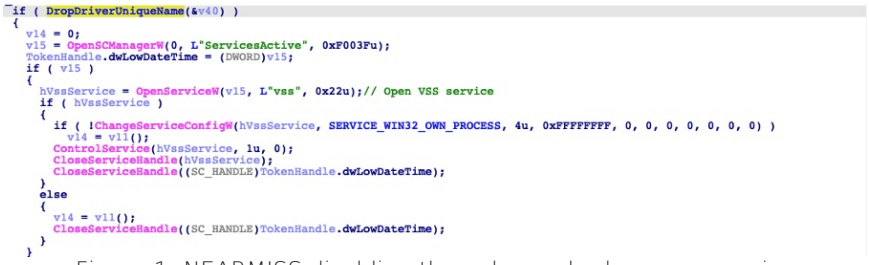
For mitigation and hardening recommendations, please review:

- Our Proactive Preparation and Hardening to Protect Against Destructive Attacks white paper
- Our Distributed Denial of Service (DDoS) Protection Recommendations white paper

Date	Target Region	Target Industry	Actor	Malware	Type of Activity	Related Reporting
Jan. 14, 2022	Ukraine	Government	Ukraine attributes defacements to UNC1151		Disruptive: defacements of Ukrainian government websites	22-00001084
Jan. 15, 2022	Ukraine	Government, Technology, Civil Society & Non-Profits	Mandiant and Ukraine attribute to UNC2589	PAYWIPE (aka WhisperGate), SHADYLOOK (aka WhisperKill)	Destructive: PAYWIPE MBR wiper disguised as ransomware	22-00001136
Feb. 15–16, 2022	Ukraine	Government, Financial Services	U.S. and UK attribute to GRU		Disruptive: DDoS	source, source, source
						22-

Feb. 23, 2022	Ukraine	Government, Financial Services			Disruptive: DDoS, defacements	00004164, 22-00004168, source
Feb. 23, 2022	Ukraine		UNC3715	NEARMISS (aka HermeticWiper, FoxBlade), PARTYTICKET (aka HermeticRansom)	Destructive: PARTYTICKET wiper disguised as ransomware allegedly deployed alongside MBR wiper NEARMISS	22-00004168, 22-00004497
Feb. 24, 2022	Ukraine	Government	APT28	NEARTWIST (aka IsaacWiper)	Destructive: wiper	22-00004605, 22-00004674, source
Feb. 24, 2022	Ukraine	Telecommunications	U.S. reportedly attributes to GRU	SKYFALL	Destructive malware caused Internet service disruptions	22-00004499, 22-00007054, 22-00008615, source, source
Feb. 27, 2022	Ukraine	Government	Possibly APT28	SDELETE	Destructive	22-00007625
March 14, 2022	Ukraine	Financial Services		CADDYWIPER	Destructive: wiper	22-00006393, source
March 16, 2022	Ukraine	Media & Entertainment		JUNKMAIL (aka DoubleZero)	Destructive: wiper	22-00007112
March 28, 2022	Ukraine	Telecommunications			Cyber incident disrupts Internet access	source, source
April 1, 2022	Ukraine	Government		CADDYWIPER	Destructive: wiper	22-00009571, source
April 8, 2022	Ukraine	Energy & Utilities		CADDYWIPER, INDUSTROYER2	Destructive and Disruptive: attempted power disruption with ICS-specific INDUSTROYER2; operation also involved IT wipers	22-00009571, 22-00009760, source, source

Table 1: Significant disruptive and destructive incidents observed during 2022 Ukraine crisis to date



```
if ( DropDriverUniqueName(&v40) )
{
  v14 = 0;
  v15 = OpenSCManagerW(0, L"ServicesActive", 0xF003Fu);
  TokenHandle.dwLowDateTime = (DWORD)v15;
  if ( v15 )
  {
    hVssService = OpenServiceW(v15, L"vss", 0x22u);// Open VSS service
    if ( hVssService )
    {
      if ( !ChangeServiceConfigW(hVssService, SERVICE_WIN32_OWN_PROCESS, 4u, 0xFFFFFFFF, 0, 0, 0, 0, 0, 0, 0) )
        v14 = v11();
      ControlService(hVssService, 1u, 0);
      CloseServiceHandle(hVssService);
      CloseServiceHandle((SC_HANDLE)TokenHandle.dwLowDateTime);
    }
    else
    {
      v14 = v11();
      CloseServiceHandle((SC_HANDLE)TokenHandle.dwLowDateTime);
    }
  }
```

Figure 1: NEARMISS disabling the volume shadow copy service

We will continue to collect reports and evidence of additional relevant incidents as information becomes available.

- Satellite internet provider ViaSat reported that a cyber event disrupted satellite internet connectivity in Ukraine and other parts of Europe, beginning on Feb. 24, 2022, and extending into March (22-00004499). ViaSat confirmed that the SKYFALL wiper, which Mandiant analysis suggests is designed to impact routers or embedded devices, was used in the incident that disrupted service to their customers (22-00008615).
- Spokespeople for Ukrainian ISP Triolan allegedly confirmed that service outages were likely linked to cyber threat activity on Feb. 24 and March 9, 2022 (22-00007054).
- Open-source reporting suggests that on Feb. 26, 2022, a wiper also affected a Ukrainian border crossing station already overwhelmed with families attempting to cross into Romania.
- On March 13, Ukrainian ISP Vinasterisk experienced a service outage, which an employee claimed was linked to a cyber incident.
- Major Ukrainian telecommunications provider Ukrtelecom reported on March 28, 2022, that it experienced a "cyber attack" resulting in disruption of Internet service to most of its users for approximately 15 hours. Ukrtelecom subsequently

reported that malicious actors accessed the company's networks using credentials of an employee in territory occupied by Russian forces.
- DDoS attacks against Ukrainian ISP McLaut apparently caused internet service disruptions for several hours on April 13, 2022.

Previous Significant Disruptive and Destructive Cyber Attacks Attributed to Russia

There is significant precedent for Russian use of disruptive and destructive cyber attacks. Most of these incidents targeted Ukraine and are likely linked to significant military or political developments, including causing power outages and influencing the outcome of elections.

- Table 2 summarizes disruptive and destructive incidents that Mandiant can attribute to Russian threat actors with at least moderate confidence based on proprietary collections and investigations as well as data released publicly by reputable sources.
- Mandiant judges that the primary objectives of most state-sponsored destructive cyber attacks include several types of strategic and tactical goals, including punishment, sabotage, compellence, testing, and signaling (19-00001539, 20-00002866, 21-00013935).
- We believe Russia's past use of disruptive and destructive attacks in Ukraine are largely consistent with objectives of sabotage, compellence, punishment, and undermining public confidence in the Ukrainian government and institutions.
- While some incidents affecting countries other than Ukraine (e.g., the TV5Monde and TRITON incidents) may reflect testing or signaling sabotage capabilities, activity targeting sports organizations and events and the Georgian election appear to be similar to punishment- or compellence-motivated activity in Ukraine.
- Threat actors leverage destructive malware to destroy data, eliminate evidence of malicious activity, or manipulate systems to cause physical impacts or render them inoperable. In some cases, these intrusions can have devastating second- and third-order effects against a larger population, such as the ETERNALPETYA (NotPetya) incident in 2017, which caused damage worldwide. Destructive cyber attacks can be a powerful means to achieve strategic or tactical objectives; however, the risk of reprisal is likely to limit the frequency of use to very select incidents. Observed destructive cyber attacks can be categorized by type: physically destructive malware, wipers, modified ransomware, and other destructive attacks (19-00001539, 20-00002866, 21-00013935).

Date	Target Region	Target Industry	Actor	Malware	Type of Activity	Notes, Possible Related Circumstances	Related Reporting
May 2014	Ukraine	Government	APT28 "CyberBerkut"		Destructive and Disruptive: vote tallying software deleted, DDoS, attempted defacement with false election results	election	Intel-1165539, 17-00000357, source
April 2015	France	Media & Entertainment	APT28 "CyberCaliphate"		Destructive and Disruptive: malware destroyed systems; broadcast interrupted		15-00005278, 16-00012858
Oct. 2015	Ukraine	Media & Entertainment	Sandworm	KILLDISK	Destructive and Disruptive: malware destroyed systems and interrupted media coverage	election	16-00003662, source, source
Dec. 2015	Ukraine	Energy & Utilities	Sandworm	KILLDISK	Destructive and Disruptive: cyber threat activity caused power outages and data destruction	possible retaliation for sabotage of power transmission towers supplying power from Ukraine to Crimea	15-00014822
Aug. 2016	Switzerland	Civil Society & Non-Profits	APT28 "@anpoland"		Disruptive: DDoS	Olympics; Russian athlete ban	18-00001642
					Destructive and Disruptive:	attacks occurred after	

Dec. 2016	Ukraine	Energy & Utilities	Sandworm	INDUSTROYER	malware caused power outages and data destruction	MH17 report accused Russia, a series of failed ceasefires and peace talks, and preceded escalation in fighting	16-00021034, 17-00006337
Dec. 2016	Ukraine	Financial Services	Sandworm	WHITEROSE	Destructive: disguised as ransomware		16-00020050
June 2017	Ukraine; global	Many	Sandworm	ETERNALPETYA	Destructive: disguised as ransomware		17-00006864, 17-00006904
Oct. 2017	Ukraine	Transportation, Media & Entertainment	Sandworm	BADRABBIT	Destructive: disguised as ransomware		17-00011900, 17-00011954
Nov. 2017	Middle East	Energy & Utilities	Temp.Veles	TRITON	Disruptive: malware designed to disable industrial safety systems, could enable physical damage		17-00014211, 18-00006335
Feb. 2018	South Korea	Civil Society & Non-Profits	Sandworm	SOURGRAPES	Destructive and Disruptive: data destruction disrupted network services before and during opening ceremonies	Olympics; Russian athlete ban	18-00002527, 18-00008982
Oct. 2019	Georgia	Media & Entertainment, Government, Telecommunications, Civil Society & Non-Profits	U.S. and UK attribute to Sandworm		Disruptive: defacements; DDoS, disruption of media broadcasts	election	19-00018530, 20-00003194

Table 2: Past Russian disruptive and destructive attacks

Additional Incidents Reported

In addition to the incidents listed above, we identified more than a dozen open-source reports describing the use of disruptive attacks in circumstances that appear to reflect Russian government interests. These incidents, summarized in Table 3, span 2002 to 2022, and reportedly affected Chechnya, Estonia, Georgia, Kyrgyzstan, Kazakhstan, Lithuania, Ukraine, Turkey, and Finland. We are unable to independently verify open-source claims or attribution to Russia for these incidents.

Date	Target Region	Target Industry	Type of Activity	Notes, Possible Related Circumstances	Related Reporting
Oct. 2002	Chechnya	Media & Entertainment	Disruptive: DDoS	active conflict, coincided with Russian advance	16-00017100, source, source
April 2007	Estonia	Government and private sector	Disruptive: DDoS	relocation of Soviet-era statue	16-00017100, source
July 2008	Georgia	Government	Disruptive: DDoS	impending invasion	16-00017100, source, source
Jan. 2009	Kyrgyzstan	Telecommunications	Disruptive: DDoS	Russian desire to close US military base	source, source
April 2009	Kazakhstan	Media & Entertainment	Disruptive: DDoS		source
Jan. 2011	Chechnya	Media & Entertainment	Disruptive: DDoS	increased tension between the Kremlin and North Caucasus militants	Intel-358780
				activity	

Jan. 2012	Lithuania	Financial Services	Disruptive: DDoS	targeted central bank	source
June 2012	Chechnya	Media & Entertainment	Disruptive: DDoS	ongoing insurgency	Intel-610544 , source
May 2013	Lithuania	Media & Entertainment	Disruptive: DDoS	possible retaliation for article accusing Russia of buying Eurovision votes	source
March 2014	Ukraine		Disruptive: DDoS	impending invasion	source, source
Dec. 2015	unnamed Baltic state	Energy & Utilities	Disruptive: DDoS	activity allegedly targeted gateway to control a Baltic energy grid	17-00009479, source
Dec. 2015	Turkey	Telecommunications	Disruptive: DDoS	possible retaliation for Turkey shooting down Russian fighter jet in Syria	16-00001092, source
April 2016	Lithuania	Government	Disruptive: DDoS	activity coincided with session to discuss Russian human rights violations in Crimea	source
April 2022	Finland	Government	Disruptive: DDoS	Finnish government websites disrupted after Finland signaled that it would seek NATO membership and during the Ukrainian President's address to Finnish parliament	source, source, source

Table 3: Additional potentially relevant disruptive and destructive attacks

Please rate this product by taking a short four question survey

Threat Intelligence Tags

Actors

- APT28
  Aliases
  - APT 28
  - APT-28
  - APT28
- UNC2589
  Aliases
  - UNC 2589
  - UNC-2589
  - UNC2589
- Sandworm Team
  Aliases
  - Sandworm Team

Affected Industries

- Civil Society & Non-profits
- Energy & Utilities
- Financial Services
- Governments
- Media & Entertainment
- Oil & Gas
- Telecommunications

- Transportation

Affected Systems

- Enterprise/Application Layer
- Safety Protection

Intended Effects

- Military Advantage
- Political Advantage
- Disruption
- Degradation
- Denial and Deception
- Destruction
- Embarrassment/Exposure/Brand Damage
- Interference with ICS

Motivations

- Military/Security/Diplomatic
- Ethnic/nationalist

Malware Families

- WHITEROSE
  Aliases
  - WHITEROSE
- INDUSTROYER
  Aliases
  - INDUSTROYER
- NEARTWIST
  Aliases
  - NEARTWIST
- CADDYWIPER
  Aliases
  - CADDYWIPER
- SHADYLOOK
  Aliases
  - SHADYLOOK
- JUNKMAIL
  Aliases
  - JUNKMAIL
- NEARMISS
  Aliases
  - NEARMISS
- PAYWIPE
  Aliases
  - PAYWIPE
- BADRABBIT
  Aliases
  - BADRABBIT
- SDELETE
  Aliases
  - SDELETE
- TRITON
  Aliases
  - TRITON
- SOURGRAPES
  Aliases
  - SOURGRAPES
- KILLDISK
  Aliases
  - KILLDISK

Source Geographies

- Belarus
- Russia

Tactics, Techniques And Procedures (TTPs)

- Malware Propagation and Deployment

Target Geographies

- France
- Georgia
- South Korea

- Switzerland
- Ukraine

Version Information

Version:10.0, April 13, 2022 05:22:44 PM

Version:11.0, May 4, 2022 08:22:09 PM

MANDIANT ADVANTAGE

This report contains content and links to content which are the property of Mandiant, Inc. and are protected by all applicable laws. This cyber threat intelligence and this message are solely intended for the use of the individual and organization to which it is addressed and is subject to the subscription Terms and Conditions to which your institution is a party. Onward distribution in part or in whole of any Mandiant proprietary materials or intellectual property is restricted per the terms of agreement. By accessing and using this and related content and links, you agree to be bound by the subscription.

©2022, Mandiant, Inc. All rights reserved.