CTI Jelentés

Wiper-ek az orosz-ukrán konfliktusban

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET

Tartalomjegyzék

Mi is az a wiper?

2022-ben vette kezdetét az orosz-ukrán konfliktus, amely során nem csak a fizikai közegben zajló háborúban jelentek meg új módszerek, hanem a kibertérben is. A dokumentum az összecsapás korai szakaszát dolgozza fel, a wiper szoftverek szemszögéből. A kialakult konfrontáció során, a világon talán először most alakult ki az eddigi legnagyobb kiberháborús harctér.

A dokumentum azt hivatott bemutatni az olvasó számára, hogy az említett kiberháború során milyen eszközökhöz, metódusokhoz folyamodtak/ folyamodnak a szemben álló felek, illetve mennyiben különböznek a megtévesztési módszerek a „lakossági" verzióktól. Az elemzés fő célja, a háború során megjelent és legtöbbet használt adattörlő kártevők, az úgynevezett „wiper" -ek megismerése.

Malware	MBR	GPT	Files	Associated Ransomware	Target OS	Languages
WhisperGate	Y	N	Y	Y	Windows	C++ (Stage 1) .NET (Stage 2, 3)
HermeticWiper	N**	N**	Y	Y	Windows	C, Assembly
IsaacWiper	Y	N**	N	N	Windows	C, C++, Assembly
DesertBlade	?	?	Y	N	Windows	Golang
ACIDRAIN*	N/A	N/A	Y	N	Linux (MIPS)	C
CaddyWiper	Y	N	Y	N	Windows	C
DoubleZero	N**	N**	Y	N	Windows	.NET
AwfulShred	Y	Y	Y	N	Linux	Bash
SoloShred	Y	Y	Y	N	Solaris	Bash

Table 1: High-level overview of each wiper's functionality (Source: Recorded Future)
** ACIDRAIN targets satellite modems, not desktop operating systems, so some fields may not be relevant.*
*** Although the MBR/GPT may be recoverable (or not affected at all), the wiper destroys the filesystem or critical files that prevent the system from successfully booting.*

A különböző wiper szoftverek jellemzői

Wipereknek nevezzük a kártevők olyan csoportját, amelyeknek a fő célja az, hogy az eszköz egész adattárolóját vagy annak meghatározott részeiről teljesen, visszaállíthatatlanul törölje a rajtalévő tartalmakat. Gyakran előfordul, hogy a wipereket zsarolóvírusnak álcázzák, azonban ezeknél a programoknál a valódi cél nem az anyagi haszonszerzés, hanem a minél gyorsabb és hatékonyabb rombolás.

A konfliktus során többször is előfordult, hogy orosz katonai műveletek előtt néhány órával már érzékelni lehetett bizonyos ukrán hálózatokon a wiperek jelenlétét. Háborús helyzetben egy ilyen taktikai lépés nagyban befolyásolhatja a fizikai harctéren történteket is. Általában megpróbálják valamilyen kulcsfontosságú létesítmény vagy intézmény hálózatára juttatni a wipert, ezért a legtöbb esetben kormányzati vagy közmű szolgáltató kerül a célkeresztbe.

A wiperek működése

A wiperek általános célja, hogy a kiszemelt számítógépen vagy számítógépeken található, bizonyos elérési útvonalakon vagy a lemez teljes egészén található adatokat visszaállíthatatlanul törölje. A wiperek tulajdonságai a főbb irányokat és célokat vizsgálva megegyeznek, azonban részleteiben sokszor különbözőek. Előfordulhat, hogy a program csak bizonyos partíció típusokat, vagy meghatározott operációs rendszereket vesz célba. A wiperek elsődlegesen az emberi hiszékenységre és megtévesztésre támaszkodnak, ezért az ilyen típusú rosszindulatú programok futtatása általában valamilyen fertőzött fájl megnyitásával kezdődnek. A kiberbűnözők hamisított e-maileket küldenek annak érdekében, hogy a felhasználók minél nagyobb arányban futtassák le az elküldött rosszindulatú fájlokat. Ahhoz, hogy ez teljesülni tudjon, az említett leveleket általában valamilyen hivatalos szerv vagy szolgáltató nevében küldik ki.

A kártevő terjesztői gyakran használják ki a konfliktus helyzetét, általában segítségnyújtással, támogatással kapcsolatos e-mailekben, tartalmakban terjednek, illetve jelennek meg. Jelenleg a háborús helyzetet próbálják kihasználni, ezért sok levél az ukrán/orosz kormány, vagy azok intézményei, szervei (védelmi minisztériumok, biztonsági szolgálatok) nevében szólítják meg a címzettet. A wiper típusától függően maga a program lefutása is különböző módokon mehet végbe. Bizonyos esetekben az e-mail-ben, vagy más módon kapott fájl lokálisan tartalmazza a wiper szoftvert. Azonban előfordultak olyan esetek is, amikor a letöltött fáj „csak" egy telepítő, amely olyan programsorokat tartalmaz, amik azért felelenek, hogy egy idegen szerverről a károkozó letöltődjön és települjön a célgépre. A megsemmisítendő adatok mennyiségétől függ, de általánosságban elmondható, hogy wiper nagyon hamar lefut, letörli az adatokat, majd a számítógép kikapcsol. Ha ezek után megpróbáljuk újraindítani a számítógépet, lehetséges, hogy már el sem fog indulni, mivel sok esetben az operációs rendszerrel együtt törlődnek az elindításához szükséges adatok is. Ha esetleg az operációs rendszer el is indul, sajnos az adatok nem lesznek elérhetők.

A wiperek főbb típusai

WhisperGate

A WhisperGate zsarolószoftver első felbukkanása 2022. január 13-án történt. A Microsoft Threat Intelligence Center (MSTIC) nem sokkal az észlelés után megkezdte a kártevő elemzését. Az MSTIC jelentése szerint, a szoftvert kifejezetten különböző ukrán szervezetek megtámadására készítették. A csoport folyamatosan vizsgál több olyan rendszert, amelyek az említett szoftver áldozatai lettek. Ezek a rendszerek főként kormányzati, illetve nagyobb informatikai rendszerek, amelyek mindegyike Ukrajnában található.

Egy esetleges fertőzés esetén a kártevő több könyvtárban is megtalálható lehet, többek között a C:\PerfLogs, C:\ProgramData, C:\, és C:\temp könyvtárakban, és az esetek többségében „stage1.exe" néven fut. A kártevő az Impacket[1] segítségével települ az adott eszközre, és felülírja az eszköz Master Boot Record (MBR)[2] partícióját egy zsarolóüzenettel.

A használt zsarolóüzenet:

„Your hard drive has been corrupted.

In case you want to recover all hard drives of your organization,You should pay us $10k via bitcoin wallet

1AVNM68gj6PGPFcJuftKATa4WLnzg8fpfv and send message via toxID

BA34F49130D0F186993C6A32DAD8976F6A5D82C1ED23054C057ECED5496F65

with your organization name.We will contact you to give further instructions."

1 Egy nyilvánosan elérhető csomaggyűjtemény, melyet hálózati protokollokkal való munkához használnak.

2 Az MBR a számítógép azon része, mely az operációs rendszer betöltéséért felelős.

A „Stage2.exe" futtatható állomány egy Discord csatornán tárolt rosszindulatú programot tölt le az áldozat eszközére. A program a rendszer egyes könyvtáraiban olyan fájlokat keres, amelyek bizonyos kiterjesztésekkel rendelkeznek.

Amennyiben egy fájlnak olyan kiterjesztése van, amit a wiper felismer, akkor a fájl kiterjesztése felülíródik a 0xCC értékkel. Érdemes felhívni a figyelmet, hogy a program nem csak a lokálisan tárolt, hanem a felcsatolt hálózati meghajtókon szereplő fájlokat is képes használhatatlanná tenni. A Microsoft Defender Antivirus és a Microsoft Defender for Endpoint már képes detektálni a WhisperGate kártevőt (felhőkörnyezetben is). A Microsoft ajánlása alapján, az esetlegesen érintett szervezetek folyamatosan monitorozzák és figyeljék a gyanús tevékenységeket, illetve ahol lehetséges engedélyezzék a többfaktoros hitelesítést (2FA). Érdemes engedélyezni a Microsoft Defender for Endpointban a „Controlled folder Access" (CFA) funkciót az MBR partíció módosításának megakadályozása érdekében.

HermeticWiper

Számos ukrajnai szervezetet ért kibertámadás, amelyet a HermeticWiper nevű új adattörlő szoftverrel végeztek el, több száz számítógépet tönkretéve, állapította meg az ESET kutatólaborja. A támadásra néhány órával azután került sor, hogy tömeges szolgáltatásmegtagadással járó (DDoS) kibertámadás ért több fontos weboldalt az országban. Az ESET termékei „Win32/KillDisk.NCV" néven azonosították a rosszindulatú szoftvert, amelyet először helyi idő szerint 2022. 02. 23-án nem sokkal délután 5 óra előtt észleltek. A program időbélyegzőjében, a 2021. december 28-ai dátum szerepel, ami arra utal, hogy a támadás már jó ideje készülhetett. A HermeticWiper felhasználja a legális „EaseUS Partition Master" partícionáló szoftver illesztőprogramjait, hogy az adatokban kárt tegyen. Az illesztőprogrammal (empntdrv.sys) visszaélve a kártevő eléri, hogy közvetlen felhasználói hozzáférést kapjon a fájlrendszerhez a Windows API-k meghívása nélkül. A támadók egy valódi tanúsítványt is használnak, amelyet egy ciprusi székhelyű, Hermetica Digital Ltd. nevű cégnek állítottak ki, innen ered a szoftver neve. A kártevő minden fizikai meghajtó első 512 bájtjának megrongálására összpontosít az MBR-ben. Bár ez már elég ahhoz, hogy az eszköz ne tudjon újraindulni, a program folytatja a partíciók formázását. A kártevő hivatkozik gyakori mappákra is (Dokumentumok, Asztal, Appdata), és a Windows eseménynapló hivatkozásai is megtalálhatóak a kódban. Egyes sorokban megtalálhatók a Windows rendszerleíró adatbázis (registry) kulcsainak módosítására írt parancsok is, hogy elősegítsék a program optimális futtatásának lehetőségét. A folyamat végén az eszköz leállását kezdeményezi, miután a parancs lefutott az eszközről minden adat törlődik.

A program a vizsgálatok nehezítésének érdekében, a folyamat legvégén saját magát is felülírja, véletlenszerűen generált bájtokkal.

ACIDRAIN

Az Acidrain olyan műholdas kapcsolatot használó modemeket céloz meg, amellyel a felhasználók az internetre képesek csatlakozni. 2022. március 1-jén egy amerikai telekommunikációs vállalat, amely nagy sebességű, szélessávú szolgáltatásokat és hálózatbiztonsági termékeket nyújt lakossági, kereskedelmi és katonai piacokon, bejelentette, hogy a műholdas internetszolgáltatások megszakadása Ukrajnában és Európa szerte, egy kibertámadás eredménye. A kimaradások egybeestek az orosz-ukrán konfliktus eseményeivel. A wiper képes többféle módszerrel is felülírni az említett modemek flash memóriáját, ezáltal használhatatlanná tenni az adott eszközt.

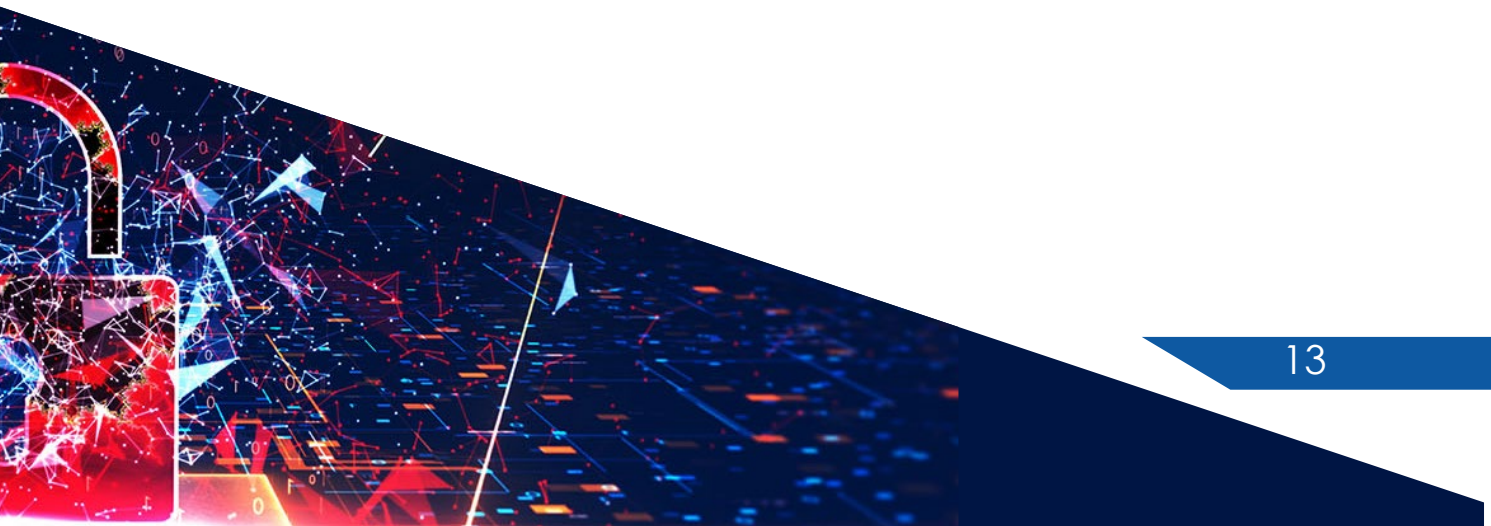
A témával kapcsolatban további érdekes információkat tudhat meg a témát feldolgozó Kibertámadás! Podcast adásunkból, illetve az NBSZ NKI egy korábbi kiberbiztonsági elemzéséből.

IsaacWiper

A támadás egy nappal az orosz katonai invázió megkezdése előtt történt. Az ESET IsaacWiper-nek keresztelte az új kártevőt, amelyet elemzésük szerint egy olyan szervezetnél detektáltak, amelyet nem érintett a korábban a HermeticWiper-rel végrehajtott támadás. A program több modult tartalmaz, van olyan, amely a kártevő hálózaton keresztüli terjesztéséért felel, illetve tartalmaz egy zsarolóvírus részt is, amely a fájlok használhatatlanná tételével foglalkozik. Az elemzések alapján több kiberbiztonsági cég is azt gondolja, hogy a program gyengébb minőségű megvalósítása miatt a HermeticWiper álcájaként használták, amolyan figyelemelterelő eszközként. Az ESET szerint nem sikerült semmi féle kézzel fogható bizonyítékot előállítani egyelőre, amely konkrét kiberbűnözői csoportokra utalna, azonban azt biztosan tudják, hogy ezeket az akciókat akár több hónapig is tervezhették. Vélhetően az Impacket és a RemCom nevű távoli hozzáférési szoftver segítségével kivitelezhették a támadást. Az IsaacWiper és a HermeticWiper között kódszintű hasonlóság nem található, kizárólag abban egyeznek, hogy a céleszközön az összes adat törlésre kerüljön.

CaddyWiper

Az ESET a CaddyWiper-t a közleményük szerint március 14-én, 09:38-kor (UTC) körül észlelték. A futtatható fájlhoz („caddy.exe") tartozó metaadatok azt mutatják, hogy a kártevőt 07:19-kor állították össze, valamivel több mint két órával az első észlelés előtt. Az ESET elemzése szerint a programban nem találtak hasonlóságot, amely a HermeticWiper és az IsaacWiperrel lehetne összeköthető, azonban a végső cél ezúttal sem változott, a felhasználói adatok és partíciós információk törlésével, minél több számítógép és hálózat működésképtelenné tétele. Az újonnan felfedezett kártevő először ellenőrzi, hogy a fertőzött számítógép tartományvezérlőként (Active Directory) működik-e. Ha nem, akkor megsemmisíti a „C:\Users" mappában található összes fájlt, majd a soron következő betűjellel azonosított meghajtóra lép és itt is törli az adatokat. A program ezt a folyamatot ismétli újra és újra, amíg le nem töröl mindent. Érdemes felhívni a figyelmet arra, hogy mivel a program a „Z" betűjellel ellátott meghajtóig törli az adatokat, veszélyeztetve vannak a fertőzött számítógéphez csatlakoztatott hálózati meghajtók is. A fájlmegsemmisítő algoritmus két szakaszból áll, az első a fájlok felülírására, a második pedig a partíciós táblák megsemmisítésére szolgál. Ez egy hatékony technika a fájlok helyreállításának nehezítésére, illetve megakadályozására.



DesertBlade

2022. március 1-jén valószínűleg orosz hackerek a DesertBlade nevű malware-t használták egy televíziós közvetítéssel foglalkozó vállalat ellen. A Microsoft jelentése szerint a malware-t ismét használták március 17. és 23. között. Az első esetben a kártevőt csoportházirend (Active Directory Group Policy) segítségével telepítették, ami azt jelzi, hogy a támadás első szakaszában az elkövetők először megszerezték az Active Directory feletti irányítást. A DesertBlade elsőként felülírja, majd törli az adott eszközön található összes állományt. A felülírás azt a célt szolgálja, hogy a visszaállítás nehezen vagy egyáltalán ne legyen lehetséges a jövőben.

DoubleZero

A DoubleZero kártevőt először 2022. március 17-én észlelték. A CERT-UA tájékoztatása szerint több „.zip" kiterjesztésű fájlt is találtak, amelyek közül az egyik a „Virus ... extremely dangerous !!!. Zip" nevet viselte. Az elemzés során a DoubleZero-t rosszindulatú törlő programnak minősítették, amelyet C# programozási nyelven fejlesztettek. A program két féle módszert használ a fájlok törlésére, az egyik, hogy 4096 bájtos nullákat tartalmazó egységekkel írja felül a meglévő adatokat, vagy pedig API hívások segítségével (NtFileOpen, NtFsControlFile (code: FSCTL_SET_ZERO_DATA)). A malware törli a következő Windows beállításjegyzékben található fájlokat is, mielőtt bezárja a fertőzött rendszert: HKCU, HKU, HKLM, HKLM \ BCD. Az esetet az „UAC-0088" azonosítóval követik nyomon.

AwfulShred

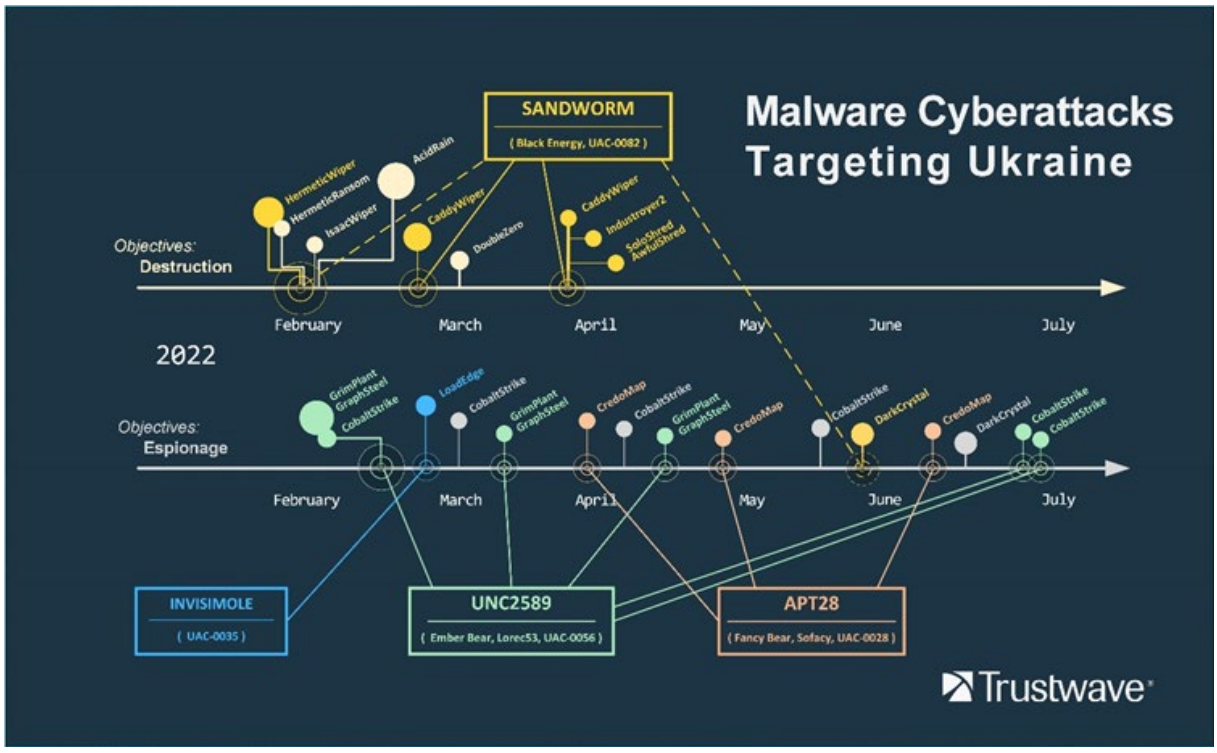
Az AwfulShred egy olyan wiper malware, amelyet kifejezetten Linux rendszerek fertőzésére fejlesztettek ki. A malware az Industroyer2 támadással függ össze, amely során az egyik ukrán energiaszolgáltatót vették célba még 2022. április elején. Az említett malware egy Bash script, amelyet az OrcShred nevű féreg terjesztett az adott infrastruktúrában található Linux operációs rendszert futtató számítógépek között. A kártevő futtatása után először a HTTP és SSH szolgáltatásokat állítja és tiltja le, majd pedig törli a /boot, /home és /var/log könyvtárak tartalmát. Végső lépésnek törli az összes csatlakoztatott meghajtót is, majd pedig újraindítja az adott eszközt. Az energiaszolgáltatót ért támadás végül sikertelen volt.

SoloShred

A SoloShred egy Bash script, amely hasonló az AwfulShred nevű malware-hez, és Solaris rendszerek tönkretételére tervezték. A kártevő leállít minden olyan szolgáltatást, amely „ssh”, „http”, „apache”, „ora_” vagy „oracle” kezdetűek. Ezután törlődnek a rendszerben található adatbázisok, majd a /boot, /home és /var/log könyvtárak tartalma, illetve az összes fájl elérési útvonala is. Minden csatlakoztatott lemez tartalma is megsemmisül, hasonlóan, mint az AwfulShred futása esetén is.

OrcShred

Az OrcShred egy féreg (worm) típusú kártevő, amely szintén a korábban már említett Industroyer2 támadás során került felfedezésre. Az OrcShred SSH felhasználásával 2 különböző wiper terjesztésére használták. A Linuxos wiper változat neve AwfulShred, a Solaris verzióé pedig SoloShred. Mivel wiperekről van szó, ezért az említett két program célja az adattárolók törlése, illetve az eszközök működésképtelenné tétele. Az OrcShred bash nyelven került implementálásra.



Idővonal az Ukrajna elleni támadókról

Kép forrása: trustwave.com

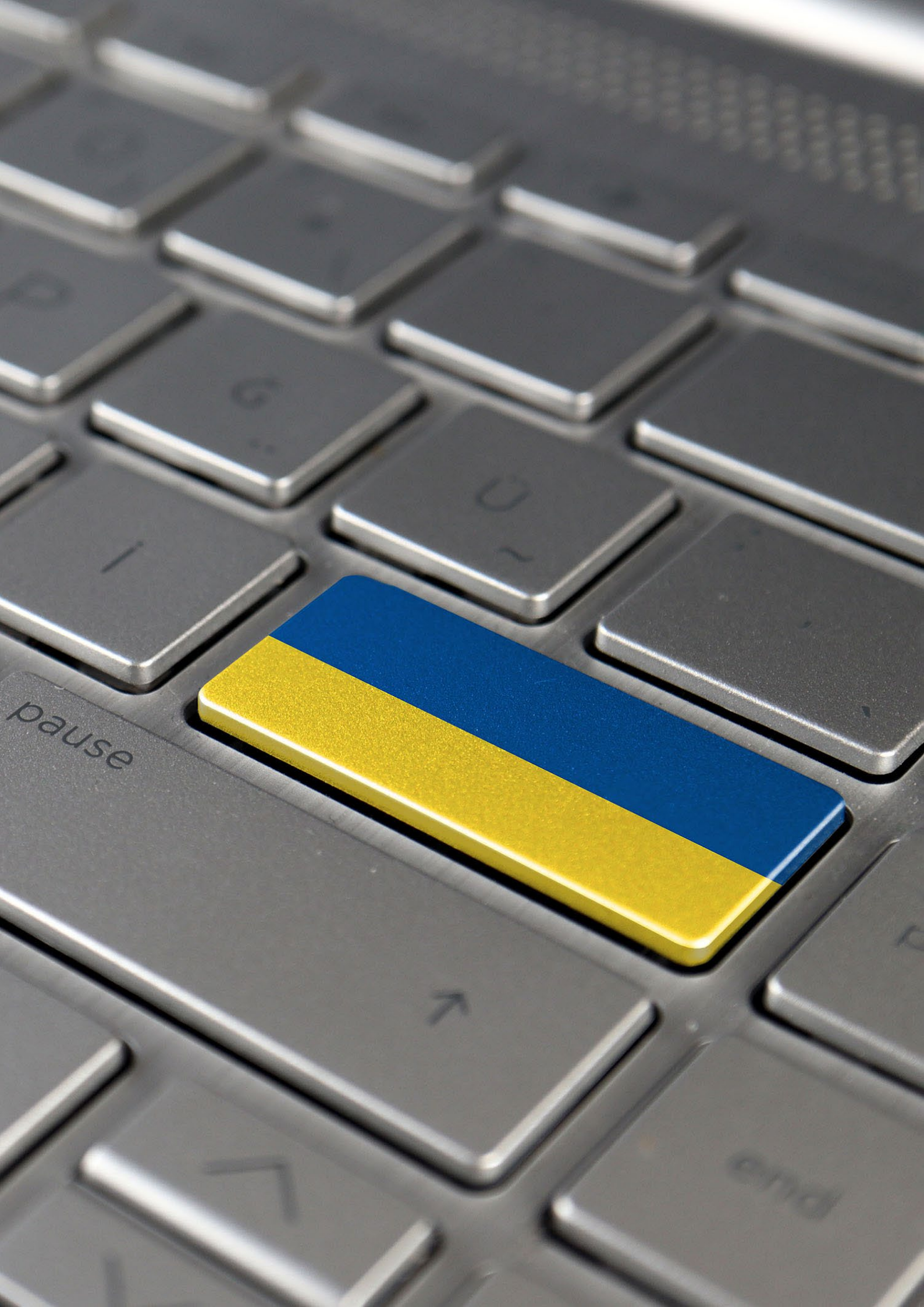
Kik állhatnak a támadások mögött?

Mint minden hasonló esetnél, itt sem lehetünk teljesen biztosak a támadók kilétét illetően. Biztonsági kutatók azonban a wiperes támadások nagy részénél a Sandworm APT csoporthoz kötötte az incidenseket. A Sandworm APT az egyik legrégebb óta figyelemmel kísért csoport, tevékenységük 2009 óta nyomon követhető. Kiberbiztonsági szakértők úgy vélik, hogy a Sandworm az orosz katonai hírszerző szolgálat (GRU) egyik alegysége lehet, ugyanis a csoport már több Oroszországgal szemben álló fél elleni támadásokban is részt vett. Az évek során több olyan rosszindulatú programot állítottak elő, amellyel hatalmas károkat tudtak okozni. Az egyik lehírhedtebb a 2016 környékén publikált NotPetya ransomware. Egyes források szerint a csoport felelős a különböző wiperek elkészítéséért is. A Sandworm hackerei már 2016-ban megtámadták az ukrán elektromos hálózatot, amelyet kifejezetten az erre a célra fejlesztett Industroyer malware segítségével hajtottak végre. 2022 áprilisában ismét megtámadták az ukrán elektromos infrastruktúrát, ezúttal az Industroyer 2-re keresztelt kártevővel, amely a korábbi Industroyer utódja.

Ukrajna hogyan védekezett a támadások ellen?

Az orosz invázió kezdetén, az orosz biztonsági szolgálatok a kritikus ukrán kormányzati adatokat vették célba. A többlépcsős invázió megkezdésekor cirkálórakéták csapódtak be egy ukrán kormányzati létesítménybe, ahol fontos adatokkal teli szerverek helyezkedtek el. Ezzel egyidejűleg orosz kiberügynökök wiper támadásokat hajtottak végre, az eszközökön megpróbálták visszaállíthatatlanul törölni az összes információt. Az orosz támadás komplex jellege ellenére az ukrán adatok túlélték a támadást. Ez csak úgy volt lehetséges, hogy azokat az adatokat, amelyeket az ukrán kormány korábban kizárólag fizikai szervereken tároltak, feltöltötték a felhőbe. A szembenállást megelőzően egy adatvédelmi törvény megtiltotta az ukrán kormánynak, hogy felhőszolgáltatást használjon az adatok tárolására és feldolgozására, így az összes adat központosított és sebezhető volt. A törvényt néhány nappal a támadás előtt módosították ahhoz, hogy engedélyezzék ugyanezen információk felhőben történő tárolását. A felhőtárolás technikájából adódóan, az adatok redundáns módon kerültek eltárolásra, így ha esetleg valamelyik szerver tönkremegy, az adatok minden további nélkül elérhetőek lesznek továbbra is.

Az orosz-ukrán kiberhelyzetről többet is megtudhat az NBSZ NKI erről szóló, Az orosz-ukrán kiberhelyzet aktualitásai [Cybersec'22] című podcast adásából.


pause

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2023