

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION**

MICROSOFT CORPORATION and
HEALTH-ISAC, INC.,

Plaintiffs,

v.

FELIX UTOMI, WAIDI SEGUN ADAMS,
and DOES 1-5,

Defendants.

Case No. 1:26-cv-3047-LMB-WEE

FILED UNDER SEAL

**ORDER GRANTING PLAINTIFFS' APPLICATION FOR A
TEMPORARY RESTRAINING ORDER AND ORDER TO
SHOW CAUSE RE: PRELIMINARY INJUNCTION**

Before the Court is Plaintiffs Microsoft Corporation's ("Microsoft") and Health-ISAC, Inc.'s Application for a Temporary Restraining Order and Order to Show Cause Re: Preliminary Injunction. Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiffs' Application, the Application is **GRANTED**. The Court hereby makes the following findings of fact and conclusions of law:

This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have personal jurisdiction over Defendants because they have purposefully availed themselves of the privilege of doing business in Virginia by: (i) victimizing 106 organizations located in Virginia; (ii) using computers and wire services physically located in Virginia and this judicial district to carry out their conduct, including Microsoft Azure hosting servers located in Microsoft's Dulles, Virginia data center; and (iii) contracting with and/or using the services of companies like Verisign, Public Interest Registry, and Cloudflare that operate in Virginia.

Microsoft® is a registered trademark owned by Microsoft, U.S. Trademark Registration No. 1,200,236. The Microsoft® mark is famous, distinctive, and widely recognized by the general consuming public of the United States as a designation of the source of goods or services.

Microsoft 365® is a registered trademark owned by Microsoft, U.S. Trademark Registration No. 6,701,693. The mark is famous, distinctive, and widely recognized by the general consuming public of the United States as a designation of the source of goods or services.

Office 365® is a registered trademark owned by Microsoft, U.S. Trademark Registration No. 4,380,754. The mark is famous, distinctive, and widely recognized by the general consuming public of the United States as a designation of the source of goods or services.

SharePoint® is a registered trademark owned by Microsoft, U.S. Trademark Registration No. 2,854,862. The mark is famous, distinctive, and widely recognized by the general consuming public of the United States as a designation of the source of goods or services.

Outlook® is a registered trademark owned by Microsoft, U.S. Trademark Registration No. 2,188,125. The mark is famous, distinctive, and widely recognized by the general consuming public of the United States as a designation of the source of goods or services.

There is good cause to believe that Defendants have engaged in and are likely to engage in future acts or practices that violate the Lanham Act (15 U.S.C. §§ 1114 et seq.); the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the Stored Communications Act (18 U.S.C. § 2701); and the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962). There is good cause to believe that Defendants are wrongfully interfering with Microsoft's contracts with its customers who are victimized by Defendants.

There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from Defendants' ongoing violations of

law. This harm will be suffered by Plaintiffs, businesses victimized by Defendants' use of stolen credentials to commit cybercrime, and the public at large.

There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective relief will result if Defendants are given the opportunity to move the EvilTokens control panel infrastructure used to operate the phishing campaigns at issue in this case to new domains before the Court's Order can be effectuated.

There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' Control Panel Domains used to operate control panels for the phishing software described in Plaintiffs' Complaint and supporting papers ("Control Panel Domains") must be immediately transferred to the control of Microsoft, where they can be secured and thus made inaccessible to Defendants. The Control Panel Domains are listed in Appendix A to this Order.

There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' Phishing Domains domains used to operate malicious websites used for the phishing operations described in Microsoft's complaint and moving papers ("Phishing Domains") must be placed on "serverHold" status or an equivalent registry-controlled prohibition that prevents the affected domains from being published in the applicable top-level-domain zone file, thereby removing their NS delegations from the authoritative TLD DNS infrastructure and causing ordinary recursive DNS resolution to fail. The Phishing Domains are listed in Appendix B to this Order.

There is good cause to direct that third party Internet registries, registrars, data centers, and hosting providers for the Control Panel Domains and Phishing Domains (collectively "Subject Domains") with a presence in the United States to reasonably assist in the implementation of this

Order and refrain from frustrating the implementation and purposes of this Order, pursuant to 28 U.S.C. § 1651(a) (the All Writs Act).

There is good cause to permit notice of the instant Order by alternative means, given the exigency of the circumstances and the need for prompt relief. Publication of a notice on the Subject Domains is reasonably calculated to notify Defendants of the instant order.

There is good cause to believe that the harm to Plaintiffs of denying the relief requested outweighs any harm to any legitimate interests of Defendants and that there is no undue burden to any third party. There is good cause to believe that the requested relief serves the public interest by protecting victims, preventing fraud, securing computer systems and electronic communications, and preserving evidence of Defendants' unlawful conduct.

NOW THEREFORE, IT IS HEREBY ORDERED that Defendants; their officers, agents, servants, employees, and attorneys; and all other persons who receive actual notice of this Order and are in active concert or participation with Defendants or their officers, agents, servants, employees, or attorneys are temporarily restrained and enjoined from:

1. Using without authorization Microsoft's trademarks and logos;
2. Gaining unauthorized access to protected computers;
3. Gaining unauthorized access to stored email communications;
4. Conducting an enterprise through a pattern of wire fraud and trademark infringement;
5. Using the Subject Domains for purposes of (i) gaining unauthorized access to computers; (ii) obtaining third party data from computers without authorization; (iii) causing harm to computers without authorization.

IT IS FURTHER ORDERED, pursuant to the All Writs Act, with respect to any of the infrastructure used to operate the Subject Domains, the owners and/or operator of such infrastructure with a presence in the United States shall take reasonable best efforts to implement the following actions:

1. Take reasonable steps to identify incoming and/or outgoing Internet traffic on their respective networks associated with Defendants that originates and/or is being sent from and/or to the Subject Domains;

2. Take reasonable steps to block incoming and/or outgoing Internet traffic on their respective networks associated with Defendants that originates and/or are being sent from and/or to the Subject Domains, by Defendants or Defendants' representatives or resellers, except as explicitly provided for in this Order;

3. Completely disable the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with Defendants' use of the Subject Domains and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives and all other persons, except as otherwise ordered herein;

4. Completely, and until further order of this Court, suspend all services to Defendants or Defendants' representatives or resellers associated with the Subject Domains;

5. Isolate and disable any content and software associated with the Defendants hosted at the Subject Domains in a manner that does not impact any content or software not associated with Defendants;

6. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this

Order is executed in full, except as necessary to communicate with hosting companies, data centers, Plaintiffs or other ISPs to execute this Order;

7. Not enable, and take all reasonable steps to prevent, any circumvention of this order by Defendants or Defendants' representatives associated with the Subject Domains including without limitation to enabling, facilitating, and/or allowing Defendants or Defendants' representatives or resellers to rent, lease, purchase, or otherwise obtain domains associated with implicated services;

8. Preserve, retain and produce to Plaintiffs all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the Subject Domains, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers and telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage, access and contact records and all records, documents and logs associated with Defendants' or Defendants' representatives';

9. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order; and

10. Completely preserve any computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the Subject Domains and preserve all evidence of any kind related to the content, data, software or accounts associated with such domains and such computer hardware, such that such evidence of Defendants' unlawful activities is preserved.

In determining the method and mechanism to disable content and software associated with the Defendants, the relevant data centers and/or hosting providers shall reasonably confer with Plaintiffs' counsel of record in this action.

IT IS FURTHER ORDERED that, pursuant to the All Writs Act, with respect to the Control Panel Domains, the domain registries with a presence in the United States shall take or cause to be taken the following actions:

1. With respect to the Control Panel Domains, within three (3) business days of receipt of this Order, or as soon as practicable, unlock and change the registrar of record for the Control Panel Domains to MarkMonitor or such other registrar specified by Microsoft. To the extent the registrar of record does not assist in changing the registrar of record for the domain under its control, the domain registry for the domain, or its administrators, including backend registry operators or administrators, within five (5) business days of receipt of this Order, or as soon as reasonably practicable, shall change, or assist in changing, the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. The purpose of this paragraph is to ensure that Microsoft has control over the hosting and administration of the domain in its registrar account at MarkMonitor or such other registrar specified by Microsoft. Microsoft shall provide to the domain registry or registrar of record any requested registrar information or account details necessary to effectuate the foregoing.

- in Appendix A 
- a. The Control Panel Domains^{in Appendix A} shall be made active and shall resolve in the manner set forth in this Order, or as otherwise specified by Microsoft, upon taking control of the Control Panel Domains;
 - b. The domain registries shall take reasonable steps to work with Microsoft to ensure the transfer of the Control Panel Domains and to ensure that Defendants cannot use the Control Panel Domains to make unauthorized access to computers, infect computers, compromise computers and computer networks, monitor the owners

and users of computers and computer networks, steal information from them or engage in any other activities prohibited by this Order;

- c. The WHOIS registrant, administrative, billing and technical contact and identifying information for the Control Panel Domains shall be modified to reflect such information as may be specified by Microsoft;
- d. Prevent transfer, modification or deletion of the Control Panel Domains by Defendants and prevent transfer or control of the Control Panel Domains to the account of any party other than Microsoft;
- e. Take all steps required to propagate the foregoing changes through the Domain Name System ("DNS"), including domain registrars.

2. With respect to the Phishing Domains, ^{in Appendix B JMB} place on "serverHold" status or an equivalent registry-controlled prohibition that prevents the affected domains from being published in the applicable top-level-domain zone file, thereby removing their NS delegations from the authoritative TLD DNS infrastructure and causing ordinary recursive DNS resolution to fail.

3. With respect to the Phishing Domains, within three (3) business days of receipt of this Order, or as soon as practicable, disable or remove associated registry-maintained DS records and in-bailiwick glue records to prevent continued delegation or DNSSEC validation of the Phishing Domains. The Phishing Domains should remain registered and locked against transfer, modification, or deletion, using appropriate statuses such as serverTransferProhibited, serverUpdateProhibited, and serverDeleteProhibited, so that registration data, operational logs, and other relevant evidence are preserved while the suspension remains in effect.

IT IS FURTHER ORDERED that copies of this Order may be served by any means authorized by law, including publication to the Control Panel Domains and via emails to the abuse contacts for the providers of the Phishing Domains.

With respect to any registrars, registries, or infrastructure providers associated with the Subject Domains that do not have a presence in the U.S. or are not otherwise subject to the Court's jurisdiction, receipt of this Order shall constitute notice that their infrastructure and/or services are being used by Defendants, and voluntary compliance with the provisions of this order is requested.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b), that the Defendants shall appear before this Court within fourteen (14) days from the date of execution of this Order, to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that Microsoft, on behalf of Plaintiffs, shall post bond in the amount of \$25,000 as cash to be paid into the Court registry.

IT IS FURTHER ORDERED that the Defendants shall file with the Court and serve on Plaintiffs' counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than two (2) days prior to the hearing on Plaintiffs' request for a preliminary injunction. Plaintiffs may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for Defendants no later than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service shall, where possible, be performed by personal or overnight delivery, facsimile or electronic communication or e-mail, and documents shall be delivered so that they shall be received by the

other parties no later than 4:00 p.m. (Eastern Time) on the appropriate dates listed in this paragraph.

IT IS SO ORDERED.

Dated: September 15, 2026



/s/ Leonie M. Brinkema
United States District Judge

APPENDIX A: CONTROL PANEL DOMAINS

redsteel.cc
yuntuoutdoorbackpack.cc
ironpeaksupply.cc
pawsprint.cc
smartbulls.org
logicnestaisolutions.org
virtualhomemakeover.org
teatimetreasures.org
5mowarriorsllc.org
kalibaitu.org
purelyelegant.org
e-commercecorner.org
puredwelling.org
clevion.org
norlume.org
joyfulworkshop.org
plushseat.org
pinkpawgo.org
asptrekgoods.org
wildwoodoutfitters.org
roamcase.org
roam-case.org
monothreads.org
wovendaily.org
knightbymyside.org
lumoshome.org
hatchelnook.org
linorallc.org
almagestshop.org
swiftdryblowdryers.org
scantechinnovations.com
smartviewdevices.com
smartframetechnologies.com
optichiplabs.com
smartlensinnovate.com
toetales.net
adaliabigllc.com
xuenoerlingeriellc.net
bayloramuse.com
crystalbrow.com
markelasoft.com
morgangentleman.com
nevorohomellc.com
kaoqumini.com
soarbox.net

campscapellc.com
trailcrownllc.com
mengchongbaotoys.com
azuresunprotectionco.com
veyramarketcollective.com

APPENDIX B: PHISHING DOMAINS

distraction.cc	6likesthiefllc.work
sunnysprouthome.cc	windcswordslc.work
cozylivingessentials.me	kaychicgear.work
urbanchicapparel.me	aiapepxsynthetica.com
victorchargellc.uk	aurorahomellc.com
katiethread.uk	cozynookfurnishings.com
bearfilmsstudio.org	bestforkitchenuse.com
adventureseekeroutfitters.org	firedimension.com
13monkeys.org	ambianceseatingboutique.com
moderncomfortpillow.org	pawglidefurmailshop.com
strongleap.org	luxurywildwood.com
urbanchicdesk.org	destinyce.com
automatelabmade.org	silkystrandswigs.com
dreamylifestyle.org	peakprooutdoorgear.com
homebliss.org	householdevents.com
zenithartistry.org	timelesstendance.com
foursgentlemenllc.org	aiinnovatehub.net
braveadventuring.org	glamourstrandsplace.com
elegancedecor.org	speedyautosupplies.com
papaleogen.org	carvibesolutions.com
timihrtfeng.org	happinessnook.com
fergusonren.org	geniusaitechnologies.com
fauxmanepalace.org	headgearhaven.com
rayonqiu.org	summitwholesalers.com
homeblissessentials.org	trendyclosetboutique.com
andreashe.org	chicthreadsboutiquellc.com
pinkrrchocolatellc.org	brennenkaisa.com
modastylehub.org	beautifulfootprints.com
salonijieson.org	yipinfurnitureshop.com
redcockscomb.org	modernmuseclothing.net
abovethesnowline.org	theurbanperch.com
himalayaoutdoor.org	luxeloft.net
investigatornyc.org	purelyclassic.net
noahenlightentech.org	modernvogueapparel.com
minemasterequipment.org	urbaneessence.com
ridgevial.org	purelyuniquely.com
mindmutt.org	blairestretch.com
neatshift.org	just-ellie.com
johnnystars.org	glitzyclothing.com
vistaframe.org	returntothemountainsandseas.com
campfold.org	princessisabe.com
stitchvibe.org	opulentthrea.com
veyraapparel.org	brighttears.com
evobothub.org	austinshan.com
nebulagoods.org	warmerjacket.com

theurbanrelaxation.com
comfortablehomesofa.com
luxeladieswardrobe.net
purelyfemmefashion.com
innovatewebdesign.net
ventureforthclothing.com
charm womens underwear.com
habitatclothing.net
yishanhui womens clothing.com
ykshark.com
timeshellselection.com
meiyazhi clothing pavilion.com
highlandforgecookware.com
veyraapparel.net
fragranthome.net
rapiddryness.com
legendaryoutdoorhikingshoes.com
sorenclothing.net
pineveileveryday.com
lumakkitchenware.com
rapiddryness.net
fancondo.com
smarterlabel.net
vastshorestylecollective.com
westridgeculinary.com
marenhomeessentials.com
zorvefashionapparel.com
shadestyles.com
duskstreetwear.net
yuedongmouse.com
mirewoodgoodsjunction.com
salinalipstickbeautyllc.com
ruikasnakersllc.com
ironpanelite.com
tabithabackpack.com
pinkpawgo.com
extraordinarytents.net
suctionsweepco.com
summittrailssupply.net
freestylefolding.com
khpkansascity.com
minimalistinsulated.com
orselaretailapex.com
elarachainjewelry.com
novabladelc.com
dariengeneraltradealliance.com

altmora.com
reedapparel.net
lumidwellingllc.com
bronzewispeedvault.com
silthreadclayspire.com
selvynmarketworks.com
lioranretailfoundry.com
rushforgefernhold.com
sycamoreforgefernward.com
bamboovesselbrasshold.com
mariswellgeneralmerchandise.com
kaironpeak.com
rustygentleman.com
jeffersonracket.com
brinsteadmarketplacepartners.com
bitesafe.net
aldenrowellc.com
driftspiregoodslc.com
hollowshaftsupplyllc.com
corvynsupplycollective.com
vorengoodsascend.com
linenspirestonecove.com
mindmutt.net
poplinloomfibercove.com
cordswift.com
cottonweftthreadcrest.com
weightedplush.net
trailtailsllc.com
luminwellmerchandisegroup.com
hempspireclayhollow.com
chiffonweftfabricward.com
silksleephavenhome.com
chipvisionoptics.com
aieditlabmade.com
alphabetalley.net
blossomcraft.net
almagestshop.com
whimsyextensionsshop.net
elegancedepartmentstore.com
petjoyboutique.com