IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

MICROSOFT CORPORATION,

Plaintiff,

v.

DOES 1-10,

Defendants.

Case No. 1:25-cv-02695-MHC

DECLARATION OF DEREK RICHARDSON RE MICROSOFT'S SUPPLEMENTAL PRELIMINARY INJUNCTION BRIEF

I, Derek Richardson, declare as follows:

1. I am a Principal Investigator in Microsoft Corporation's Digital Crimes Unit ("DCU"). I make this declaration based upon my personal knowledge, and upon information and belief from my review of documents and evidence collected during Microsoft's investigation into the matters described below.

2. I am one of the persons at Microsoft primarily responsible for investigating the conduct of Defendants described in Microsoft's complaint in this case as it relates to the Lumma malware.

3. Upon issuance of the Court's temporary restraining order ("TRO") on May 15, 2025, Microsoft commenced efforts to execute the TRO by notifying relevant third-party Internet Service Providers of the TRO. At the same time, law enforcement agencies in the United States and Europe undertook their own actions to disrupt Lumma malware marketplace infrastructure in the U.S. and abroad.

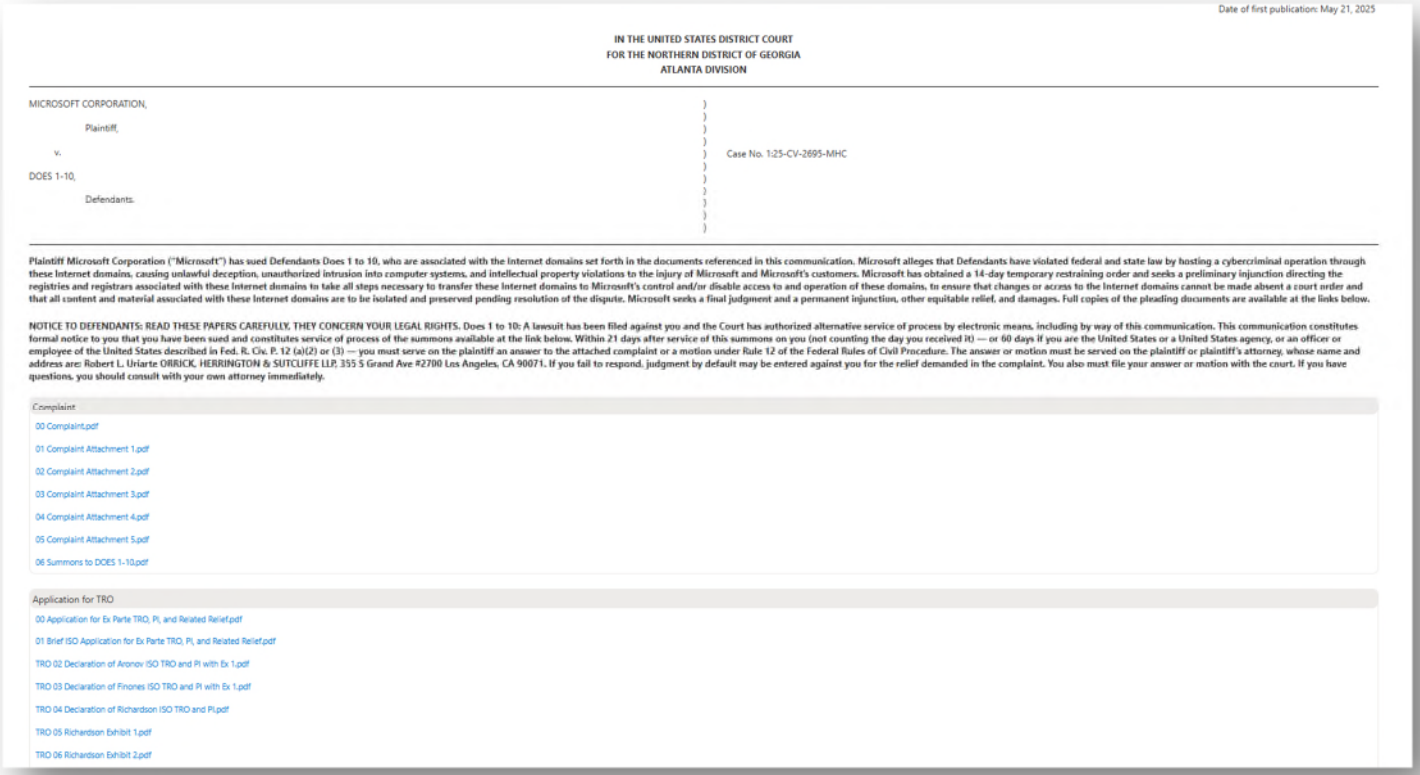
4. The TRO, Microsoft's actions, the actions of Microsoft's private partners, and the actions of U.S. and foreign law enforcement agencies succeeded in causing a significant disruption of Defendants ability to distribute Lumma malware and victimize computers infected with Lumma malware. Although at least one Defendant has continued their malicious activities, they have been effectively forced off U.S. infrastructure and are now operating primarily through a small number of domains provided by Russian ISPs. The number of active command-and-control domains ("C2 domains") has been reduced by an order of magnitude, with only approximately two active domains being observed per day in the wake of the TRO. Redirection of victim computer traffic away from Defendants' prior C2 infrastructure and to Microsoft's sinkhole has yielded valuable threat intelligence enabling Microsoft to continue to monitor and act on new infrastructure as well as identify victims targeted by those behind Lumma thereby beginning the victim notification and remediation process.

5. I understand from evidence gathered in aftermath of the TRO that Defendants received notice of this case and the seizure of Defendants' malicious domains pursuant to the TRO. For example, Defendants attempted to circumvent the efforts of Microsoft and law enforcement by moving certain infrastructure to ISPs located outside of the U.S.

6. It is my belief that Defendants likely learned of this case from some combination of the notice message published to seized domains and from various national and international press publications discussing this case. Figure 1 below is the notice message Defendants would have encountered upon trying to visit any of the seized domains, and Figure 2 below shows the Microsoft pleadings notice website (https://www.noticeofpleadings.net/lumma/index.html) linked in the notice message:

Figure 1

Figure 2



Date of first publication: May 21, 2025

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

MICROSOFT CORPORATION,
Plaintiff,
v.
DOES 1-10,
Defendants.

Case No. 1:25-CV-2695-MHC

Plaintiff Microsoft Corporation ("Microsoft") has sued Defendants Does 1 to 10, who are associated with the Internet domains set forth in the documents referenced in this communication. Microsoft alleges that Defendants have violated federal and state law by hosting a cybercriminal operation through these Internet domains, causing unlawful deception, unauthorized intrusion into computer systems, and intellectual property violations to the injury of Microsoft and Microsoft's customers. Microsoft has obtained a 14-day temporary restraining order and seeks a preliminary injunction directing the registries and registrars associated with these Internet domains to take all steps necessary to transfer these Internet domains to Microsoft's control and/or disable access to and operation of these domains, to ensure that changes or access to the Internet domains cannot be made absent a court order and that all content and material associated with these Internet domains are to be isolated and preserved pending resolution of the dispute. Microsoft seeks a final judgment and a permanent injunction, other equitable relief, and damages. Full copies of the pleading documents are available at the links below.

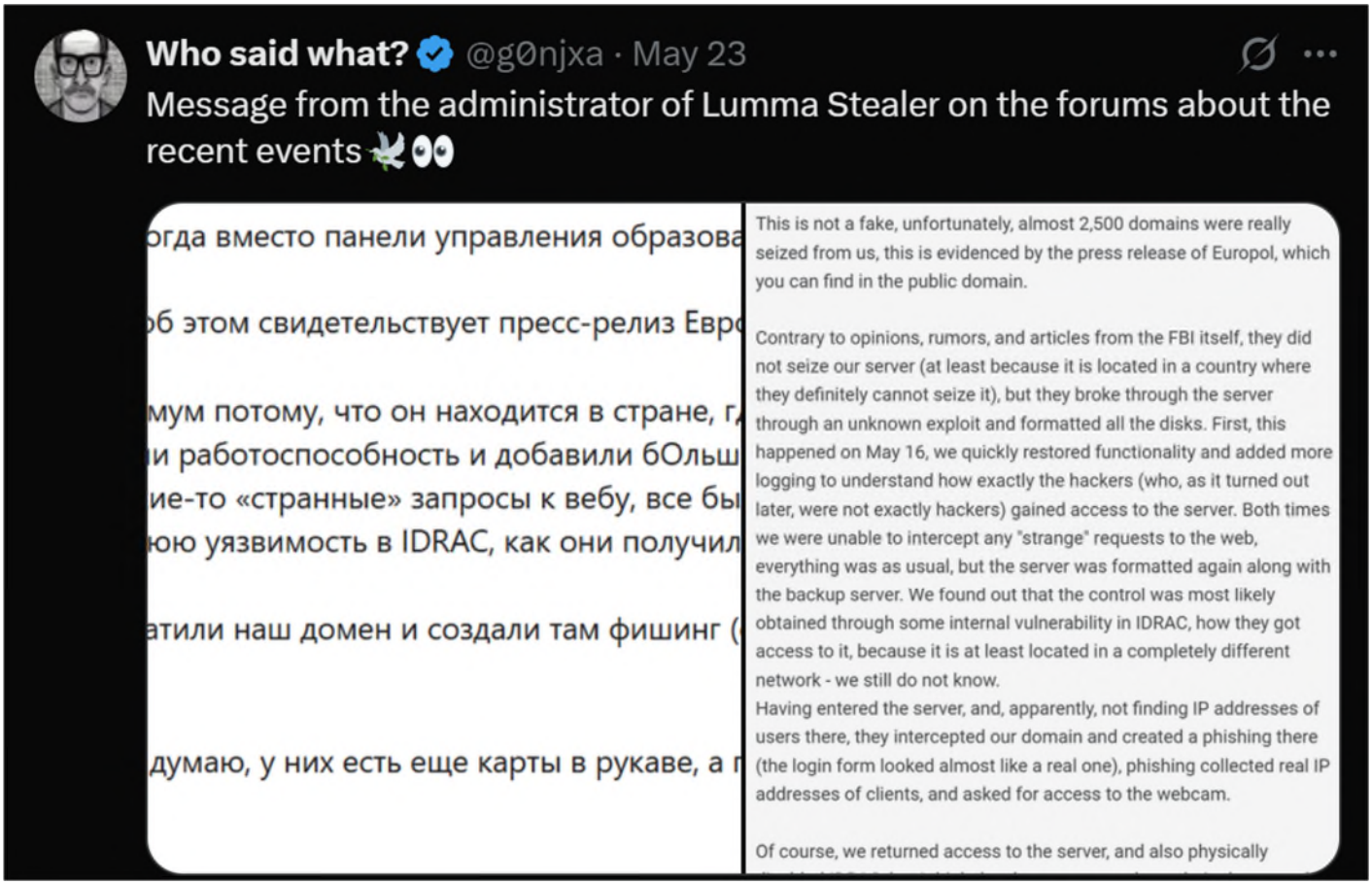
NOTICE TO DEFENDANTS: READ THESE PAPERS CAREFULLY, THEY CONCERN YOUR LEGAL RIGHTS. Does 1 to 10: A lawsuit has been filed against you and the Court has authorized alternative service of process by electronic means, including by way of this communication. This communication constitutes formal notice to you that you have been sued and constitutes service of process of the summons available at the link below. Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: Robert L. Uriarte ORRICK, HERRINGTON & SUTCLIFFE LLP, 355 S Grand Ave #2700 Los Angeles, CA 90071. If you fail to respond, judgment by default may be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court. If you have questions, you should consult with your own attorney immediately.

Complaint
00 Complaint.pdf
01 Complaint Attachment 1.pdf
02 Complaint Attachment 2.pdf
03 Complaint Attachment 3.pdf
04 Complaint Attachment 4.pdf
05 Complaint Attachment 5.pdf
06 Summons to DOES 1-10.pdf

Application for TRO
00 Application for Ex Parte TRO, PI, and Related Relief.pdf
01 Brief ISO Application for Ex Parte TRO, PI, and Related Relief.pdf
TRO 02 Declaration of Aronov ISO TRO and PI with Ex 1.pdf
TRO 03 Declaration of Finones ISO TRO and PI with Ex 1.pdf
TRO 04 Declaration of Richardson ISO TRO and PI.pdf
TRO 05 Richardson Exhibit 1.pdf
TRO 06 Richardson Exhibit 2.pdf

7. I am informed and believe based on Microsoft's investigation to date that DOE 1, aka "Shamel," released a statement on social media discussing Lumma disruption efforts, as depicted in Figure 3 below. A true and correct of the post on the social media platform "X" depicted in Figure 3 is attached to this declaration as Exhibit 1.

Figure 3



8. Attached to this declaration as Exhibit 2 is a true and correct copy of a May 21, 2025 press release published by the U.S. Department of Justice discussing Lumma malware disruption efforts, located at the URL https://www.justice.gov/opa/pr/justice-department-seizes-domains-behind-major-information-stealing-malware-operation

9. Attached to this declaration as Exhibit 3 is a true and correct copy of a May 21, 2025 press release published by Europol's European Cybercrime Centre

discussing Lumma malware disruption efforts, located at the URL https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world%E2%80%99s-largest-infostealer-lumma

10. Attached to this declaration as Exhibit 4 is a true and correct copy of a May 21, 2025 Microsoft blog discussing this case and the Lumma malware, located at the URL https://blogs.microsoft.com/on-the-issues/2025/05/21/microsoft-leads-global-action-against-favored-cybercrime-tool/

11. Attached to this declaration as Exhibit 5 is a true and correct copy of a USA Today article discussing this case and the Lumma malware, available at the URL https://www.usatoday.com/story/tech/2025/05/21/microsoft-lumma-malware-windows-computers/83771957007/

12. Attached to this declaration as Exhibit 6 is a true and correct copy of a Reuters article discussing this case and the Lumma malware, available at the URL https://www.reuters.com/sustainability/boards-policy-regulation/microsoft-files-legal-action-against-information-stealing-malware-lumma-stealer-2025-05-21/

13. Attached to this declaration as Exhibit 7 is a true and correct copy of a CNBC article discussing this case and the Lumma malware, available at the URL https://www.cnbc.com/2025/05/21/microsoft-malware-windows.html

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge, information, and belief. Executed this 10th day of June, 2025 at Redmond, Washington.

Derek Richardson

EXHIBIT 1

← **Post**

Who said what? ✓
@g0njxa

Message from the administrator of Lumma Stealer on the forums about the recent events 🕊️👀

огда вместо панели управления образова
об этом свидетельствует пресс-релиз Евро
мум потому, что он находится в стране, г
и работоспособность и добавили бОльш
ие-то «странные» запросы к вебу, все бы
ою уязвимость в IDRAC, как они получил
атили наш домен и создали там фишинг (
думаю, у них есть еще карты в рукаве, а г

This is not a fake, unfortunately, almost 2,500 domains were really seized from us, this is evidenced by the press release of Europol, which you can find in the public domain.

Contrary to opinions, rumors, and articles from the FBI itself, they did not seize our server (at least because it is located in a country where they definitely cannot seize it), but they broke through the server through an unknown exploit and formatted all the disks. First, this happened on May 16, we quickly restored functionality and added more logging to understand how exactly the hackers (who, as it turned out later, were not exactly hackers) gained access to the server. Both times we were unable to intercept any "strange" requests to the web, everything was as usual, but the server was formatted again along with the backup server. We found out that the control was most likely obtained through some internal vulnerability in IDRAC, how they got access to it, because it is at least located in a completely different network - we still do not know.
Having entered the server, and, apparently, not finding IP addresses of users there, they intercepted our domain and created a phishing there (the login form looked almost like a real one), phishing collected real IP addresses of clients, and asked for access to the webcam.

Of course, we returned access to the server, and also physically

Who said what? ✓ @g0njxa · May 22
Apparent new message from LE about the Lumma Stealer situation 👇👇
x.com/g0njxa/status/...

азательств! Мы не можем дождаться, ч
manowork вышлет новые домены для
ших коллегах - подписчиках или админи
ummaC2
нформацией... в том числе и админы.

We have a lot of evidence to process! We can't wait to review it all with you.

We're also looking forward to @lummanowork sending out new domains for the panels.

Again, if you have information about your fellow Lumma subscribers or admins, you can reach us at:

Telegram: t.me/FBILummaC2 or @FBILummaC2
Signal: +1 202-270-5371

6:22 AM · May 23, 2025 · **22.3K** Views

I would like to technically clarify the situation that happened a couple of days ago, when instead of the control panel, the page "this website has been seized" appeared.

This is not a fake, unfortunately, almost 2,500 domains were really seized from us, this is evidenced by the press release of Europol, which you can find in the public domain.

Contrary to opinions, rumors, and articles from the FBI itself, they did not seize our server (at least because it is located in a country where they definitely cannot seize it), but they broke through the server through an unknown exploit and formatted all the disks. First, this happened on May 16, we quickly restored functionality and added more logging to understand how exactly the hackers (who, as it turned out later, were not exactly hackers) gained access to the server. Both times we were unable to intercept any "strange" requests to the web, everything was as usual, but the server was formatted again along with the backup server. We found out that the control was most likely obtained through some internal vulnerability in IDRAC, how they got access to it, because it is at least located in a completely different network - we still do not know.
Having entered the server, and, apparently, not finding IP addresses of users there, they intercepted our domain and created a phishing there (the login form looked almost like a real one), phishing collected real IP addresses of clients, and asked for access to the webcam.

Of course, we returned access to the server, and also physically disabled IDRAC, but I think they have more cards up their sleeve, and so we will soon return with a new statement :)

See you soon!

Хотелось бы технически прояснить ситуацию, которая произошла пару дней назад, когда вместо панели управления образовалась страница «this website has been seized».

Это не фейк, к сожалению, у нас действительно изъяли почти 2500 тысячи доменов, об этом свидетельствует пресс-релиз Европола который Вы можете найти в открытом доступе.

Вопреки мнениям, слухам, и статьям от самого ФБР у нас не изъяли сервер (как минимум потому, что он находится в стране, где его точно не смогут изъять), однако пробили сервер через неизвестный эксплоит и форматировали все диски. Сначала, это произошло 16 мая, мы быстро восстановили работоспособность и добавили бОльше логирования, чтобы понять, как именно хакеры (которые как потом выяснилось не совсем хакеры) получили доступ к серверу. Оба раза нам не удалось перехватить какие-то «странные» запросы к вебу, все было как обычно, однако сервер вновь был форматирован вместе с сервером бэкапов. Мы выяснили, что управление скорее всего было получено через какую то внутреннюю уязвимость в IDRAC, как они получили к нему доступ, ведь он как минимум находится совсем в другой сети - нам не известно до сих пор.
Зайдя на сервер, и, видимо, не обнаружив там IP-адресов пользователей они перехватили наш домен и создали там фишинг (форма входа выглядела почти как настоящая), фишинг собирал реальные IP-адреса клиентов, и просил доступ к веб-камере.

Доступ к серверу мы, разумеется, вернули, так же физически отключили IDRAC, но, я думаю, у них есть еще карты в рукаве, а по этому скоро вернемся с новым заявлением 🙂

До скорого!

EXHIBIT 2

PRESS RELEASE

Justice Department Seizes Domains Behind Major Information-Stealing Malware Operation

Wednesday, May 21, 2025

For Immediate Release

Office of Public Affairs

Coordinated Microsoft Actions and Court-Authorized Domain Seizures Disrupt LummaC2 Malware Infrastructure Used to Target Millions Worldwide

The Justice Department announced today the unsealing of two warrants authorizing the seizure of five internet domains used by malicious cyber actors to operate the LummaC2 information-stealing malware service.

“The Department will continue to use its unique tools, authorities, and partnerships to disrupt malicious cyber operations and criminal networks,” said Sue J. Bai, head of the Justice Department’s National Security Division. “Today’s disruption is another instance where our prosecutors, agents, and private sector partners came together to protect us from the persistent cybersecurity threats targeting our country. We are grateful for their work and dedication.”

“Malware like LummaC2 is deployed to steal sensitive information such as user login credentials from millions of victims in order to facilitate a host of crimes, including fraudulent bank transfers and cryptocurrency theft,” said Matthew R. Galeotti, head of the Justice Department’s Criminal Division. “Today’s announcement demonstrates that the Justice Department is resolved to use court-ordered disruptions like this one to protect the public from the theft of their personal information and their assets. The Department is also committed to working with and appreciates the efforts of the private sector to safeguard the public from cybercrime.”

“The FBI is committed to disrupting the key services that cyber criminals rely on,” said Assistant Director Bryan Vorndran of FBI’s Cyber Division. “That’s why, with our partners, we took action against the most popular infostealer service available in online criminal markets, which is responsible for millions of attacks against victims. Thanks to partnerships with the private sector, we were able to disrupt the LummaC2 infrastructure and seize user panels. Together, we are making it harder, and more painful, for cyber criminals to operate.”

As alleged in the affidavits filed in support of the government’s seizure warrants, the administrators of LummaC2 used the seized websites to distribute LummaC2, an information-stealing malware, to their affiliates and other cyber criminals. According to court documents, common targets for cybercriminals using malware like LummaC2 include browser data, autofill information, login credentials for accessing email and banking services, as well as cryptocurrency seed phrases, which permit access to virtual currency wallets. As alleged in the affidavits, the FBI has identified at least 1.7 million instances where LummaC2 was used to steal this type of information.

The government’s affidavit further alleges that the seized domains, also referred to as user panels, served as login pages for the LummaC2 malware, allowing credentialed users and administrators to access and deploy LummaC2. On May 19, 2025, the government seized two domains. On May 20, 2025, as detailed in court documents, the LummaC2 administrators informed their users of three new domains that they had set up to host the user panel. The next day, the government then seized those three domains.

The seizure of these domains by the government will prevent the owners and cybercriminals from using the websites to access LummaC2 to compromise computers and steal victim information. Individuals who now visit the websites will see a message indicating that the site has been seized by the Justice Department, including the FBI.

Concurrent with today’s actions and consistent with the Department’s approach to public-private operational coordination, Microsoft announced an independent civil action to take down 2,300 internet domains also claimed to be used by the LummaC2 actors or their proxies.

FBI’s Dallas Field Office is investigating the case.

The U.S. Attorney's Office for the Northern District of Texas, the National Security Division's National Security Cyber Section, and the Criminal Division's Computer Crime and Intellectual Property Section are handling the case.

The U.S. Department of State's Rewards for Justice (RFJ) program, which is administered by the Diplomatic Security Service, offers a reward of up to $10 million for information on foreign government-linked individuals participating in certain malicious cyber activities against U.S. critical infrastructure in violation of the Computer Fraud and Abuse Act.

Anyone with information on any other foreign government-linked malicious cyber actors or activity targeting U.S. critical infrastructure should contact Rewards for Justice via the RFJ Tor-based tip line at: he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion (Tor browser required). Learn more about Rewards for Justice and their reward offers at RewardsforJustice.net.

If you believe you have a compromised computer or device, please visit the FBI's Internet Crime Complaint Center (IC3). You may also contact your local FBI field office directly.

Updated May 21, 2025

Topics

CYBERCRIME | NATIONAL SECURITY

Components

Criminal Division | Criminal - Computer Crime and Intellectual Property Section | Federal Bureau of Investigation (FBI) | National Security Division (NSD) | USAO - Texas, Northern

Press Release Number: 25-535

Related Content

PRESS RELEASE

Five Men Plead Guilty for Their Roles in Global Digital Asset Investment Scam Conspiracy Resulting in Theft of More than $36.9 Million from Victims

Five men have pleaded guilty for their roles in laundering more than $36.9 million from victims of an international digital asset investment scam conspiracy that was carried out from scam...

June 9, 2025

PRESS RELEASE

Department Files Civil Forfeiture Complaint Against Over $7.74M Laundered on Behalf of the North Korean Government

The Department of Justice filed a civil forfeiture complaint today in the U.S. District Court for the District of Columbia alleging that North Korean information technology (IT) workers obtained illegal...

June 5, 2025

PRESS RELEASE

Federal Jury Convicts Pakistani Weapons Smuggler of Transporting Iranian Advanced Conventional Weapons Destined for the Houthis in Yemen

A federal jury convicted a Pakistani national today on charges related to smuggling Iranian-made advanced conventional weaponry destined for the Houthis in Yemen and threatening multiple witnesses.

June 5, 2025

Office of Public Affairs
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington DC 20530

Office of Public Affairs Direct Line
202-514-2007

Department of Justice Main Switchboard
202-514-2000

EXHIBIT 3

NEWS

Europol and Microsoft disrupt world's largest infostealer Lumma

Public-private partnerships are a cornerstone of Europol's work in the digital age

Publish date21 May 2025

Europol's European Cybercrime Centre has worked with Microsoft to disrupt Lumma Stealer ("Lumma"), the world's most significant infostealer threat.

This joint operation targeted the sophisticated ecosystem that allowed criminals to exploit stolen information on a massive scale. Europol coordinated with law enforcement in Europe to ensure action was taken, leveraging intelligence provided by Microsoft.

Between 16 March and 16 May 2025, Microsoft identified over 394 000 Windows computers globally infected by the Lumma malware. In a coordinated follow-up operation this week, Microsoft's Digital Crimes Unit (DCU), Europol, and international partners have disrupted Lumma's technical infrastructure, cutting off communications between the malicious tool and victims. In addition, over 1 300 domains seized by or transferred to Microsoft, including 300 domains actioned by law enforcement with the support of Europol, will be redirected to Microsoft sinkholes.

The Head of Europol's European Cybercrime Centre, Edvardas Šileris, said: "This operation is a clear example of how public-private partnerships are transforming the fight against cybercrime. By combining Europol's coordination capabilities with Microsoft's technical insights, a vast criminal infrastructure has been disrupted. Cybercriminals thrive on fragmentation – but together, we are stronger."

What is Lumma?

Lumma, the world's largest infostealer, was a sophisticated tool that enabled cybercriminals to collect sensitive data from compromised devices on a massive scale. Stolen credentials, financial data, and personal information were harvested and sold through a dedicated marketplace, making Lumma a central tool for identity theft and fraud worldwide.

The Lumma marketplace operated as a hub for buying and selling the malware, providing criminals with user-friendly access to advanced data-stealing capabilities. Its widespread use and accessibility made it a preferred choice for cybercriminals looking to exploit personal and financial data.

A coordinated response across the world

Europol acted as the central point in Europe for intelligence sharing and coordination. After receiving critical intelligence from Microsoft, Europol's European Cybercrime Centre enriched this information and provided Member States with a view of the threat landscape to ensure a clear understanding of the network's operations.

Acting as a facilitator for Member States, Europol played a crucial role in deconfliction, ensuring that overlapping investigations were identified and managed effectively. By gathering all relevant intelligence and making sure that impacted Member States received the necessary information promptly, Europol enabled a quick response.

In a coordinated move, the United States Department of Justice (DOJ) seized the Lumma control panel, which was critical to the Lumma marketplace.

Microsoft's collaboration with Japan's Cybercrime Control Center (JC3) also led to the suspension of Lumma infrastructure based in Japan, further dismantling the criminal network.

Delivering security through partnerships

This operation demonstrates Europol's strategy of delivering security through public-private partnerships, a cornerstone of its approach to combating crime in the digital age. In an increasingly interconnected world, the fight against cyber threats cannot be won by law enforcement alone.

Public-private partnerships allow Europol to bridge the gap between the private sector's technical expertise and law enforcement's operational capabilities. By leveraging the strengths of each, Europol can deliver more impactful results, disrupting cybercriminal operations at their core.

The cooperation with Microsoft in this operation was carried out under Article 26 of Europol's Regulation, which allows Europol to receive information from and collaborate with private parties for the prevention and combat of serious crime.

Microsoft is a member of Europol's Advisory Group on Internet Security.

Read Microsoft's announcement here.

Tags

Crime areas: Cybercrime • High-Tech crime Services: Operational coordination • Operational support • Information exchange • Analysis • Operational • Intelligence • Mobile office Document type: Press Release/News Article type: Press Release Participating Countries: United States • Japan Entities: European Cybercrime Center (EC3) Operations: Other Organisations: Microsoft

EXHIBIT 4

Disrupting Lumma Stealer: Microsoft leads global action against favored cybercrime tool

May 21, 2025 | Steven Masada - Assistant General Counsel, Microsoft's Digital Crimes Unit

Microsoft's Digital Crimes Unit (DCU) and international partners are disrupting the leading tool used to indiscriminately steal sensitive personal and organizational information to facilitate cybercrime. On Tuesday, May 13, Microsoft's DCU filed a legal action against Lumma Stealer ("Lumma"), which is the favored info-stealing malware used by hundreds of cyber threat actors. Lumma steals passwords, credit cards, bank accounts, and cryptocurrency wallets and has enabled criminals to hold schools for ransom, empty bank accounts, and disrupt critical services.

Via a court order granted in the United States District Court of the Northern District of Georgia, Microsoft's DCU seized and facilitated the takedown, suspension, and blocking of approximately 2,300 malicious domains that formed the backbone of Lumma's infrastructure. The Department of Justice (DOJ) simultaneously seized the central command structure for Lumma and disrupted the marketplaces where the tool was sold to other cybercriminals. Europol's European Cybercrime Center (EC3) and Japan's Cybercrime Control Center (JC3) facilitated the suspension of locally based Lumma infrastructure.

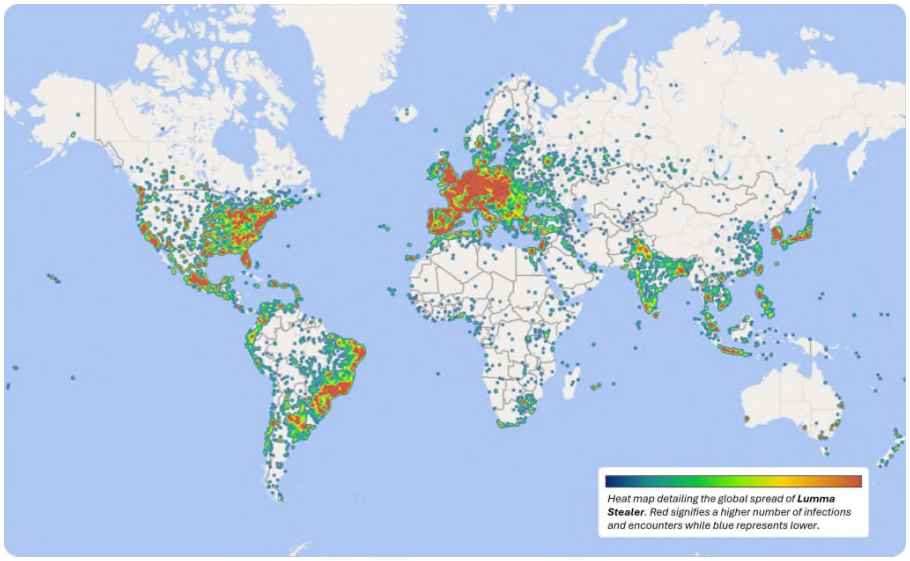
Between March 16, 2025, and May 16, 2025, Microsoft identified over 394,000 Windows computers globally infected by the Luma malware. Working with law enforcement and industry partners, we have severed communications between the malicious tool and victims. Moreover, more than 1,300 domains seized by or transferred to Microsoft, including 300 domains actioned by law enforcement with the support of Europol, will be redirected to Microsoft sinkholes. This will allow Microsoft's DCU to provide actionable intelligence to continue to harden the security of the company's services and help protect online users. These insights will also assist public- and private-sector partners as they continue to track, investigate, and remediate this threat. This joint action is designed to slow the speed at which these actors can launch their attacks, minimize the effectiveness of their campaigns, and hinder their illicit profits by cutting a major revenue stream.

More Cybersecurity Stories

Digital Crimes Unit: Leading the fight against cybercrime >
May 3, 2022

Keeping your vote safe and secure: A story from inside the 2020 election >
June 22, 2021

'It's about doing the right thing' – A tech diplomat on democracy and what motivates him >
May 7, 2021



Heat map detailing global spread of Lumma Stealer malware infections and encounters across Windows devices.

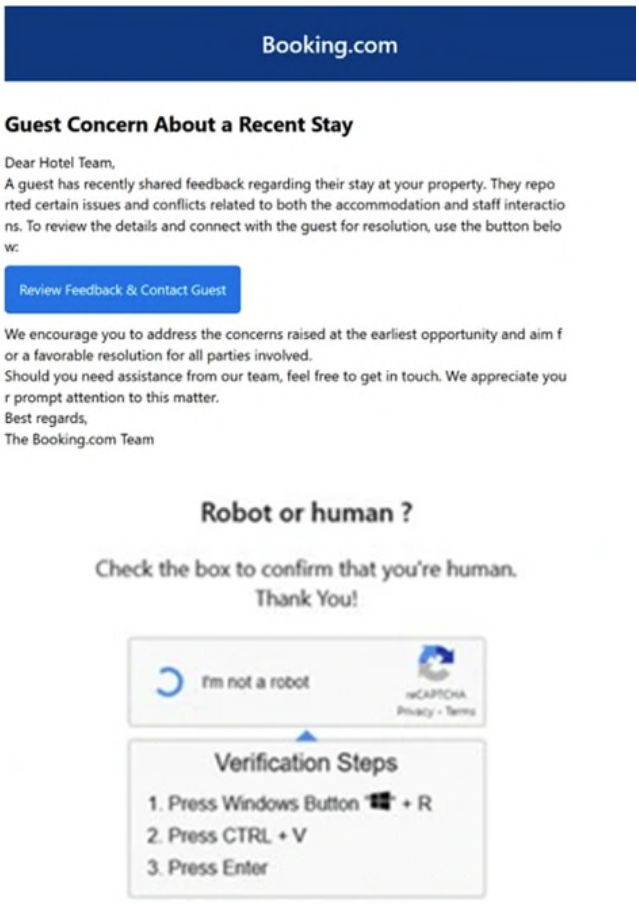
Splash page displayed on 900+ domains seized by Microsoft.

What is Lumma?

Lumma is a Malware-as-a-Service (MaaS), marketed and sold through underground forums since at least 2022. Over the years, the developers released multiple versions to continually improve its capabilities. Microsoft Threat Intelligence shares more details around the delivery techniques and capabilities of Lumma in a recent blog.

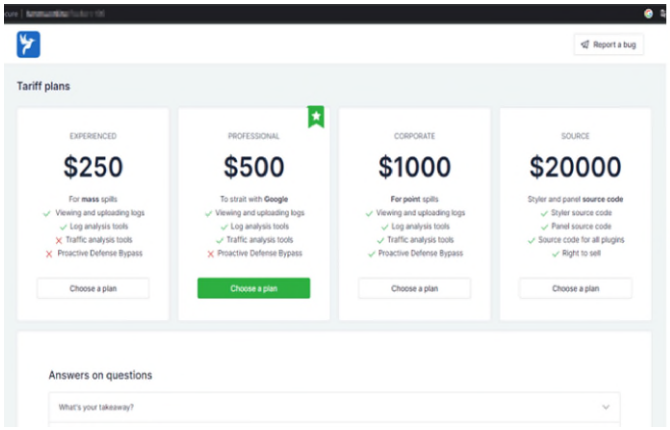
Typically, the goal of Lumma operators is to monetize stolen information or conduct further exploitation for various purposes. Lumma is easy to distribute, difficult to detect, and can be programmed to bypass certain security defenses, making it a go-to tool for cybercriminals and online threat actors, including prolific ransomware actors such as Octo Tempest (Scattered Spider). The malware impersonates trusted brands, including Microsoft, and is deployed via spear-phishing emails and malvertising, among other vectors.

For example, in March 2025, Microsoft Threat Intelligence identified a phishing campaign impersonating online travel agency Booking.com. The campaign used multiple credential-stealing malware, including Lumma, to conduct financial fraud and theft. Lumma has also been used to target gaming communities and education systems and poses an ongoing risk to global security, with reports from multiple cybersecurity companies outlining its use in attacks against critical infrastructure, such as the manufacturing, telecommunications, logistics, finance, and healthcare sectors.



Example of phishing email impersonating Booking.com and fake CAPTCHA verification prompt. (Source:Microsoft – Phishing campaign impersonates Booking .com, delivers a suite of credential-stealing malware)

The primary developer of Lumma is based in Russia and goes by the internet alias "Shamel." Shamel markets different tiers of service for Lumma via Telegram and other Russian-language chat forums. Depending on what service a cybercriminal purchases, they can create their own versions of the malware, add tools to conceal and distribute it, and track stolen information through an online portal.



Different tiers of service for Lumma, as well as Lumma's logo used on marketing material. (Source: Darktrace – The Rise of MaaS & Lumma Info Stealer)

In an interview with cybersecurity researcher "g0njxa" in November 2023, Shamel shared that he had "about 400 active clients." Demonstrating the evolution of cybercrime to incorporate established business practices, he effectively created a Lumma brand, using a distinctive logo of a bird to market his product, calling it a symbol of "peace, lightness, and tranquility," and adding the slogan "making money with us is just as easy."

Shamel's ability to operate openly underscores the importance for countries worldwide to address the issue of safe havens and to advocate for the rigorous enforcement of due diligence obligations under international law.

Continuing to work together to disrupt prolific cybercrime tools

Disrupting the tools cybercriminals frequently use can create a significant and lasting impact on cybercrime, as rebuilding malicious infrastructure and sourcing new exploit tools takes time and costs money. By severing access to mechanisms cybercriminals use, such as Lumma, we can significantly disrupt the operations of countless malicious actors through a single action.

Continued collaboration across industry and government remains imperative. We are grateful for the partnership with others across government and industry, including cybersecurity companies ESET, Bitsight, Lumen, Cloudflare, CleanDNS, and GMO Registry. Each company provided valuable assistance by quickly taking down online infrastructure.

Finally, we know cybercriminals are persistent and creative. We, too, must evolve to identify new ways to disrupt malicious activities. Microsoft's DCU will continue to adapt and innovate to counteract cybercrime and help ensure the safety of critical infrastructure, customers, and online users.

Organizations and individuals can protect themselves from malware like Lumma by using multi-factor authentication, running the latest anti-malware software, and being cautious with attachments and email links. More information for security professionals can be found here.

Tags: cyberattacks, cybersecurity, Microsoft Digital Crimes Unit, The Digital Crimes Unit

EXHIBIT 5

USA TODAY

TECH Microsoft Add Topic +

Microsoft says it squashed malware that infected 394,000 Windows computers

Kathryn Palmer
USA TODAY

May 21, 2025, 3:29 p.m. ET

Microsoft said on Wednesday, May 21 its Digital Crimes Unit partnered with law enforcement and cybersecurity agencies to disrupt an information-stealing malware that infected hundreds of thousands of Windows computers in the last two months.

The unit filed a legal action against Lumma Stealer last week after it found 394,000 Windows computers globally infected with the malware between March 16 and May 16, Windows said in a statement on its blog, calling it a "favored" malware used by criminals to steal passwords, credit cards, bank accounts and cryptocurrency wallets.

"Typically, the goal of Lumma operators is to monetize stolen information or conduct further exploitation for various purposes," Microsoft said. "Lumma is easy to distribute, difficult to detect, and can be programmed to bypass certain security defenses, making it a go-to tool for cybercriminals and online threat actors."

Cybersecurity: FBI says these 13 old internet routers are vulnerable to attacks. Is yours on the list?

The investigative unit helped in the "takedown, suspension, and blocking of malicious domains that formed the backbone of Lumma's infrastructure," after it was granted a court order by the U.S. District Court of the Northern District of Georgia, the blog said.

The U.S. Department of Justice assisted, Microsoft said, taking control of Lumma's central command structure and disrupting the marketplaces where the tool was sold. Europol's European Cybercrime Center and Japan's Cybercrime Control Center also aided in dismantling Lumma infrastructure, which has "severed communications between the malicious tool and victims," according to the blog post.

The Department of Justice said on Wednesday it seized five internet domains used by malicious cyber actors to operate the Lumma malware service. The FBI's Dallas Field Office is investigating the case, according to Reuters.

"The growth and resilience of Lumma Stealer highlight the broader evolution of cybercrime and underscores the need for layered defenses and industry collaboration to counter threats," Microsoft said in a separate blog post on the malware.

Contributing: Reuters.

Kathryn Palmer is a national trending news reporter for USA TODAY. You can reach her at kapalmer@usatoday.com and on X @KathrynPlmr.

EXHIBIT 6

Microsoft files legal action against information-stealing malware Lumma Stealer

reuters.com/sustainability/boards-policy-regulation/microsoft-files-legal-action-against-information-stealing-malware-lumma-stealer-2025-05-21

Reuters May 21, 2025

A view shows a Microsoft logo at Microsoft offices in Issy-les-Moulineaux near Paris, France, March 21, 2025. REUTERS/Gonzalo Fuentes/File Photo Purchase Licensing Rights, opens new tab

(MSFT.O), opens new tab said on Wednesday its Digital Crimes Unit (DCU) filed a legal action against Lumma Stealer last week, after it found nearly 400,000 Windows computers globally infected by the information-stealing malware in the past two months.
Lumma is capable of stealing data from various browsers and applications, such as cryptocurrency wallets, and installing other malware, the company said in a blog.

Make sense of the latest ESG trends affecting companies and governments with the Reuters Sustainable Switch newsletter. Sign up here.

Microsoft's DCU helped in the "takedown, suspension, and blocking of malicious domains that formed the backbone of Lumma's infrastructure," via a court order from the U.S. District Court of the Northern District of Georgia, the blog said.

The U.S. Department of Justice said on Wednesday it has seized five internet domains used by malicious cyber actors to operate the LummaC2 information-stealing malware service. The FBI's Dallas Field Office is investigating the case.

"The growth and resilience of Lumma Stealer highlight the broader evolution of cybercrime and underscores the need for layered defenses and industry collaboration to counter threats," Microsoft said in a separate blog post on the malware.

Reporting by Juby Babu in Mexico City; Editing by Alan Barona

EXHIBIT 7

Microsoft takes down Lumma Stealer malware network

cnbc.com/2025/05/21/microsoft-malware-windows.html

Jonathan Vanian May 21, 2025

Key Points

- Microsoft said Wednesday that it broke down the Lumma Stealer malware project with the help of law enforcement officials across the globe.
- Hackers used the malware to steal passwords, credit cards, bank accounts and cryptocurrency wallets.
- The U.S. Department of Justice took control of Lumma's "central command structure" and squashed the online marketplaces where bad actors purchased the malware.

Windows 11 operating system logo is displayed on a laptop screen for illustration photo.

Beata Zawrzel | Nurphoto | Getty Images

Microsoft said Wednesday that it broke down the Lumma Stealer malware project with the help of law enforcement officials across the globe.

The Lumma malware was a favorite hacking tool used by bad actors, Microsoft said in the post. Hackers used the malware to steal passwords, credit cards, bank accounts and cryptocurrency wallets.

The tech giant said in a blog post that its digital crimes unit discovered more than 394,000 Windows computers were infected by the Lumma malware worldwide between March 16 through May 16.

Microsoft said its digital crimes unit was able to dismantle the web domains underpinning Lumma's infrastructure with the help of a court order from the U.S. District Court for the Northern District of Georgia.

The U.S. Department of Justice then took control of Lumma's "central command structure" and squashed the online marketplaces where bad actors purchased the malware.

The cybercrime control center of Japan "facilitated the suspension of locally based Lumma infrastructure," the blog post said.

"Working with law enforcement and industry partners, we have severed communications between the malicious tool and victims," Microsoft said in the post. "Moreover, more than 1,300 domains seized by or transferred to Microsoft, including 300 domains actioned by law enforcement with the support of Europol, will be redirected to Microsoft sinkholes."

Microsoft said that other tech companies like Cloudflare, Bitsight and Lumen also helped break down the Lumma malware ecosystem.

Hackers have been buying the Lumma malware via underground online forums since at least 2022, all while developers were "continually improving its capabilities," the blog post said.

The malware has become the "go-to tool for cybercriminals and online threat actors" because it's easy to spread and break through some security defenses with the right programming, the company said.

In one example of how criminals used Lumma, Microsoft pointed to a March 2025 phishing campaign in which bad actors misled people into believing they were part of the Booking.com online travel service.

These cybercriminals used the Lumma malware to carry out their financial crimes in this scheme, the company said.

Additionally, Microsoft said that hackers have used Lumma to attack online gaming communities and education systems, while other cybersecurity companies have noted that the malware has been used in cyberattacks targeting manufacturing, logistics, health care and other related critical infrastructure.

.