Operation Endgame: Do Takedowns and Arrests Matter?

By James Shank

Published: 2025-06-17 · Archived: 2026-04-05 22:36:06 UTC

4 Min Read

Source: wsf AL via Alamy Stock Photo

COMMENTARY

On April 9, 2025, Operation Endgame announced the detention of five people. These arrests target the customers of the criminals arrested in 2024, during the first Operation Endgame. The initial effort provided the evidence for this new round of arrests.

Operation Endgame is an international effort to tackle cybercrime, involving cooperation between several countries' federal law enforcement agencies, with functional support from Europol. This includes several EU member states, as well as the US, Canada, and the United Kingdom. First becoming public in 2024, Operation Endgame now attempts to raise the costs on threat actors by seizing criminal resources, unmasking actor identities, and making arrests.

Operation Endgame is far from the first effort like this. It's also not the only effort like this going on right now. This raises the question: Do efforts like Operation Endgame work? Do these efforts matter, and is their impact visible?

Related:Automotive Cybersecurity Threats Grow in Era of Connected, Autonomous Vehicles

An answer is emerging for the larger-picture question. For defenders to be successful, we have to change the economics of security, implement cost on the actor's side, and rebalance the equation.

Takedowns and coordinated law enforcement activities have a long history of activity. Assessing past takedown activities surrounding Emotet and Trickbot, as well as the Operation Endgame targets, can give us an understanding of the impact of these efforts.

The Most Significant Cybersecurity Threat in the World

Emotet was first detected in 2014 and grew to become the most significant cybersecurity threat in the world by 2021. Emotet was primarily used to send malicious spam and functioned as a botnet of controlled victim devices.

In January 2021, Emotet was the target of a large coordinated takedown involving an exceptionally large number of public and private sector participants. This effort offered the first signs of proof that large coordinated takedowns of this scale could make a lasting impact. The actors behind Emotet tried to resurrect the botnet several times following the takedown. The next couple of years saw some Emotet activity, but always at significantly reduced rates and with much less impact. Eventually, the actors abandoned Emotet altogether.

Trickbot was first reported in October 2016. The Trickbot and Emotet crews had a long-running underground business relationship. Emotet offered loader services to Trickbot before Trickbot incorporated its own loader functionality in 2018. Later, when Emotet tried to rebuild, they used Trickbot as a loader service. Trickbot itself became the target of choice for a collaborative takedown effort in late 2020. This effort was led by US Cyber Command and Microsoft. US Cyber Command exploited features of Trickbot to neuter the malware, while Microsoft went to court. Microsoft sued on the grounds that Trickbot was illegally distributing Microsoft's code by including components of Microsoft's software development kit (SDK). This created a future legal basis for some powerful companies to pursue disruption efforts against malware by leveraging copyright enforcement with hosting providers and ISPs to take down criminal services.

Related:Critical Flaw in Langflow AI Platform Under Attack

Operation Endgame became public in 2024, after the voids of Emotet and Trickbot created space for other malicious tools to surge. The first takedown effort, now known as Season 1, took place in April 2024, targeting several gangs and malware infrastructures.

Smokeloader was significantly affected by the takedown. Pikabot and IcedID were affected but, by some accounts, were still functioning shortly after the Season 1 takedown. Bumblebee was affected, only coming back later in 2024. The effect on each of these targets ended up either being the direct end of that strain of malware or significantly degrading the functionality of the malware.

Related:Patch Now: Oracle's Fusion Middleware Has Critical RCE Flaw

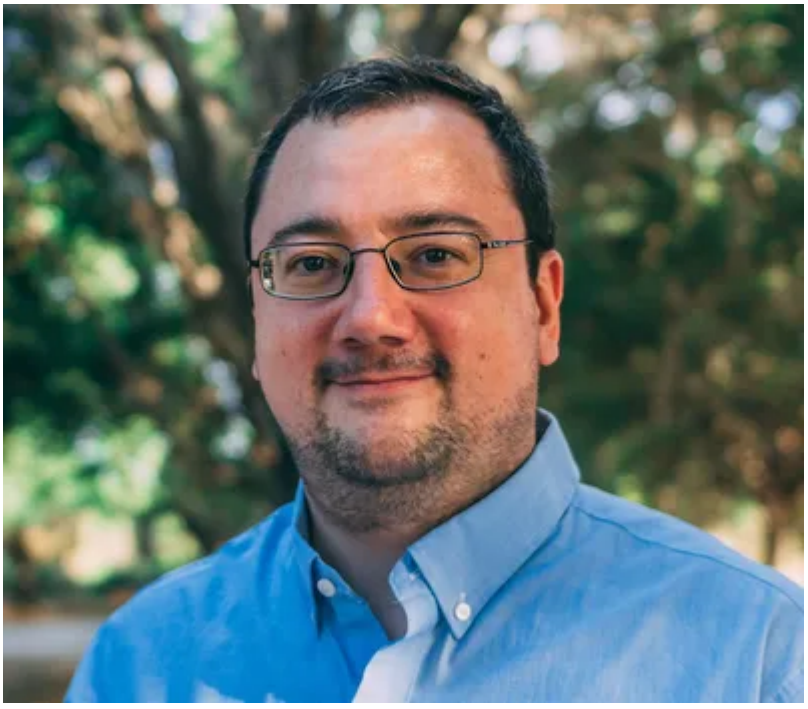
Cybercrime Will Always Exist

Now we are in Season 2 of Operation Endgame and see another round of detentions of criminals, this time the customers of Smokeloader. The message is clear: Law enforcement is still pursuing the cybercriminals and their associates more than a year after the initial action.

Are these takedown efforts effective? The clear answer is yes. They are changing the game for cybercriminals, slowing down the attacks, and giving the defenders some breathing room. Cybercrime will never fully be defeated — no one has any false hopes that takedowns will ever lead to a world without cybercrime. Yet these efforts have resulted in a world with a little less cybercrime, if only for a time.

Cybercrime response needs more aggressive actions from those seeking to protect victims and pursue criminals. What, then, should we pursue? Everything. Everywhere. All at once. And always. This is not a battle; this is a war that will continue for as long as humankind has electronic devices. And for as long as that remains true, defenders will need coordinated takedowns to shift the costs onto the adversaries and remind them that they are not safe from law enforcement efforts.

About the Author



Director, Threat Operations, Expel

James Shank is director of threat operations at Expel, where he’s responsible for threat intelligence, vulnerability intelligence, and threat hunting. He also serves as chair of the board for Internet Fire Brigade Society, a non-profit focused on bringing lasting solutions to Internet security problems outside of the remit of for-profit organizations. James is passionate about keeping the needs of the Internet information security community at the center of his efforts by being involved and coordinating several community-oriented efforts to combat online threats.

Source: https://www.darkreading.com/vulnerabilities-threats/operation-endgame-takedowns-arrests-matter