ESET takes part in global Operation Endgame to disrupt Amadey botnet and Stealc infostealer

DUBAI , DUBAI, UNITED ARAB EMIRATES, June 29, 2026 /EINPresswire.com/ -- ESET Research assisted in disrupting the Amadey botnet and the Stealc infostealer by providing technical analysis, infrastructure tracking, and affiliate-level insights. Both are operated as malware as a service (MaaS). The operation – coordinated by Microsoft Digital Crimes Unit (DCU), BitSight, Lumen, and Mitsui Bussan Secure Directions (MBSD) – targeted all known network infrastructure used by Amadey and Stealc affiliates in order to cripple their cybercriminal operations. At the same time, Europol's European Cybercrime Centre (EC3), together with European law enforcement partners, including Germany's Federal Criminal Police Office, and both the Dutch and Danish National Police, were investigating Stealc as part of Operation Endgame, alongside IBM and Proofpoint.

The ESET telemetry detection rate indicates that Amadey was observed globally without a specific regional focus. The highest detection rates were observed in India, Turkey, Egypt, Mexico, and Spain. Stealc, too, was distributed globally without a specific regional focus. The highest detection rates were observed in the United States, Poland, and Italy.

ESET contributed to the disruption by providing technical analysis, statistical information, known command and control (C&C) servers, encryption keys, campaign and build identifiers, and other threat intelligence collected during our long-term tracking of both malware families.

"ESET has been tracking both Amadey botnet and Stealc infostealer for the past three years. For the disruption operation, we shared statistics covering Q4 2025 to H1 2026, along with technical indicators and configuration data extracted from processed malware samples," explains ESET researcher Jakub Tomanek, who assisted in the Amadey and Stealc disruption efforts. "Our automated systems have been dissecting Amadey and Stealc samples and identifying the fields

most relevant for large-scale tracking. These include C&C servers, build identifiers, encryption keys, URL paths, campaign identifiers, and other embedded values used by the malware families during communication with attacker-controlled infrastructure," he adds.

Sharing technical analysis, statistical information, and threat intelligence, such as C&C server lists, affiliate identifiers, and encryption keys, enables law enforcement agencies to identify, prioritize, and act against infrastructure with a high degree of confidence.

Amadey is a modular malware loader. Its main purpose is to distribute additional malware to compromised systems, although it also offers modules for data exfiltration and remote access. Stealc, in contrast, is typical infostealer as a service. It targets credentials, cookies, cryptocurrency wallets, browser extensions, and files matching affiliate-defined patterns.

Both malware families are sold as services and advertised on darknet forums. In both ecosystems, affiliates receive a self-hosted administration panel that must be deployed on their own server infrastructure. This requires a certain level of technical skill from affiliates, and gives them direct control over victim data and payload distribution.

While distribution methods ultimately depend on each individual affiliate, ESET telemetry consistently showed that both malware families were delivered through a wide range of channels. The most common methods included fake software updates, cracked software installers, and third-party malware loaders.

Amadey used a pay-per-rebuild model. Affiliates purchased a license and then paid an additional fee each time they needed to generate a new build (for example, when rotating to a new C&C server). In other words, Amadey operators did not provide affiliates with a builder tool; instead, samples were compiled on request for each affiliate. It offers three modules for further data exfiltration and access: a clipboard monitoring module, a credential theft module, and a VNC-based remote access module. The service is priced at USD 600 in Bitcoin for a single license, with an additional USD 50 charged per rebuild.

Stealc took a more affiliate-friendly approach, offering unlimited build generation as part of the subscription. This lowered the operational cost of rotating C&C infrastructure and made it easier for affiliates to generate new samples as needed. It targets a broad range of data sources, including credentials stored by web browsers, email clients, FTP clients, gaming platforms, cryptocurrency wallet files, and browser extensions. Stealc is sold as a monthly subscription with the cheapest subscription for 1,000 USD per six months.

Trying to avoid impersonation scams, both operators explicitly instructed prospective affiliates on darknet forums to contact them only through official channels. Amadey directed buyers to private messages on the darknet forum where it is advertised, while Stealc used private messages on darknet forums or Telegram.

ESET will continue to monitor both families and track any attempts to rebuild operational infrastructure following the disruption.

For more details about Amadey and Stealc disruption, check out the ESET Research blogpost, "ESET takes part in global operation to disrupt Amadey and Stealc," on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X), BlueSky, and Mastodon for the latest news from ESET Research.

About ESET
ESET® provides cutting-edge cybersecurity to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of emerging global cyberthreats, both known and unknown—securing businesses, critical infrastructure, and individuals. Whether it's endpoint, cloud, or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. The ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit www.eset.com or follow our social media, podcasts, and blogs.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here