ZEROFOX INTELLIGENCE

Flash

New DanaBot Malware Variant Emerges After Takedown

F-2025-11-14a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Malware, Threat Actor, Ransomware

November 14, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 8:00 AM (EST) on November 14, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | New DanaBot Malware Variant Emerges After Takedown

| Key Findings

- On November 10, 2025, security researchers observed a new variant of DanaBot malware—six months after a law enforcement operation removed 300 servers and 650 domains that were used as part of the DanaBot network infrastructure.
- Unlike previous iterations of DanaBot, the new variant reportedly harnesses standard IP-based command and control (C2) domains and dark web addresses to facilitate delivery of other modules and configuration files, enabling enhanced persistence and continuous execution.
- The re-emergence of DanaBot indicates that disrupted cybercrime networks are very likely to reorganize under recognizable branding to reignite their criminal enterprises as long as financial incentives persist.

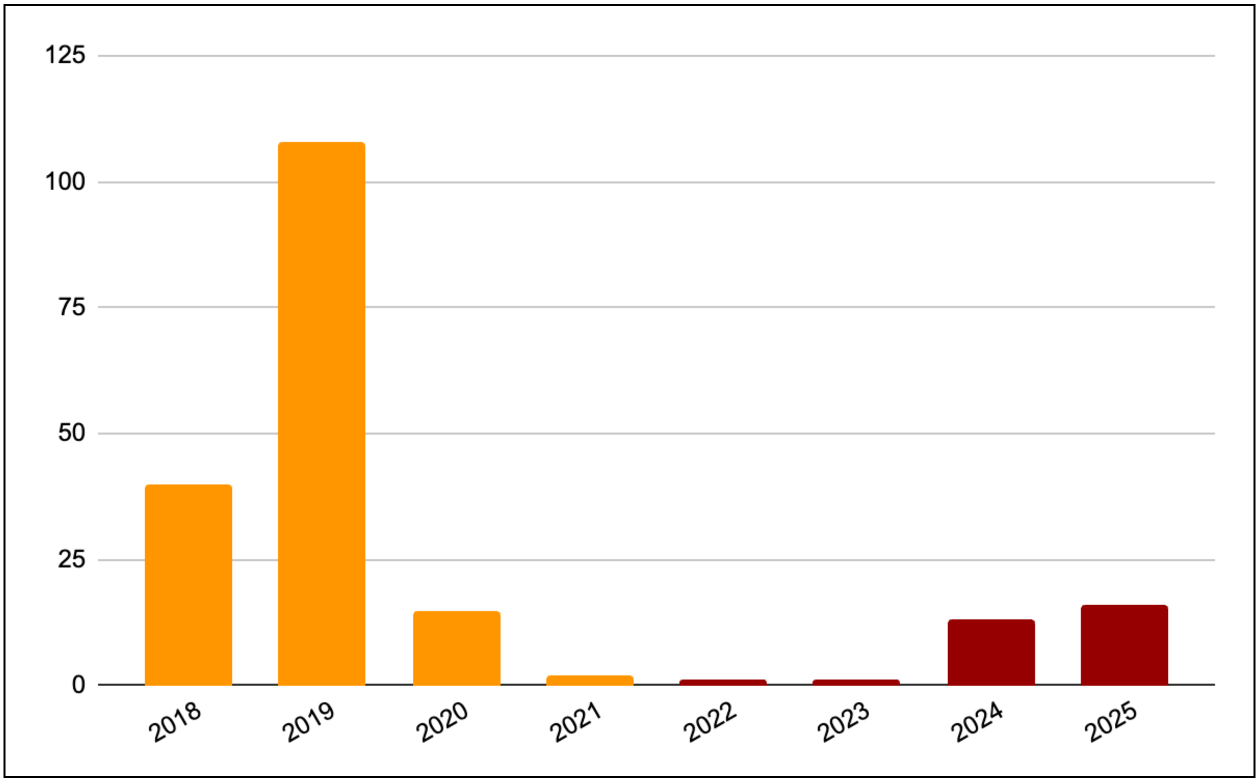
Details

On November 10, 2025, security researchers observed a variant of DanaBot malware dubbed "version 669"—six months after a law enforcement operation removed 300 servers and 650 domains that were used as part of the DanaBot network infrastructure.[1] The takedown, referred to as Operation Endgame, was a U.S.-led, international law enforcement effort to disrupt the notorious cybercriminal network.

DanaBot is a malware-as-a-service (MaaS) first identified in 2018. During its initial deployment period between 2018–2020, DanaBot was used as a banking trojan—an attack type that was the most popular email-based malware threat at the time. Throughout this period, DanaBot was delivered by several prominent cybercrime actors, before nearly disappearing from the threat landscape for three years. Typical initial access methods observed at that time in DanaBot included:

- Malicious emails (via links or attachments)
- Search engine optimization (SEO) poisoning
- Malvertising campaigns, some of which led to ransomware

[1] hXXps://www.bleepingcomputer[.]com/news/security/danabot-malware-is-back-to-infecting-windows-after-6-month-break/



DanaBot attacks per year 2018–2025

Source:
hXXps://www.proofpoint[.]com/us/blog/threat-insight/brief-history-danabot-longtime-ecrime-juggernaut-disrupted-operation-endgame

Upon its first return in December 2023, DanaBot had evolved into a modular information stealer and loader that targeted credentials and cryptocurrency stored in web browsers. Banking trojan activity had decreased during this period, with a corresponding increase in malware focused on botnets, loaders, and information stealers as precursors to ransomware payloads.

Development of DanaBot has been widely attributed to “Scully Spider”. The U.S. Cybersecurity & Infrastructure Security Agency (CISA) has identified Scully Spider as a likely Russia-based initial access broker and cybercriminal group that often conducts attacks that support Russian interests but is not part of the Russian government-controlled cyber espionage infrastructure.[2]

[2] hXXps://www.cisa[.]gov/news-events/cybersecurity-advisories/aa22-110a

Unlike previous iterations of DanaBot, version 669 harnesses standard IP-based C2 domains and dark web addresses to facilitate delivery of other modules and configuration files, enabling enhanced persistence and continuous execution.[3] This emphasis on stealth and persistence likely makes this variant a more significant threat than previous iterations of DanaBot. The new structure of C2 in version 669 indicates the developers have completely rebuilt their infrastructure from the ground up, reinventing DanaBot into a highly persistent threat to financial institutions, cryptocurrency assets, and individual users. Core functionalities of version 669 reportedly include:

- Modular plugin-based credential theft from browsers
- File Transfer Protocol clients (likely for post-exfiltration data transfer)
- Email applications
- Pre-transmission RC4 compression and encryption of exfiltrated data to avoid packet inspection

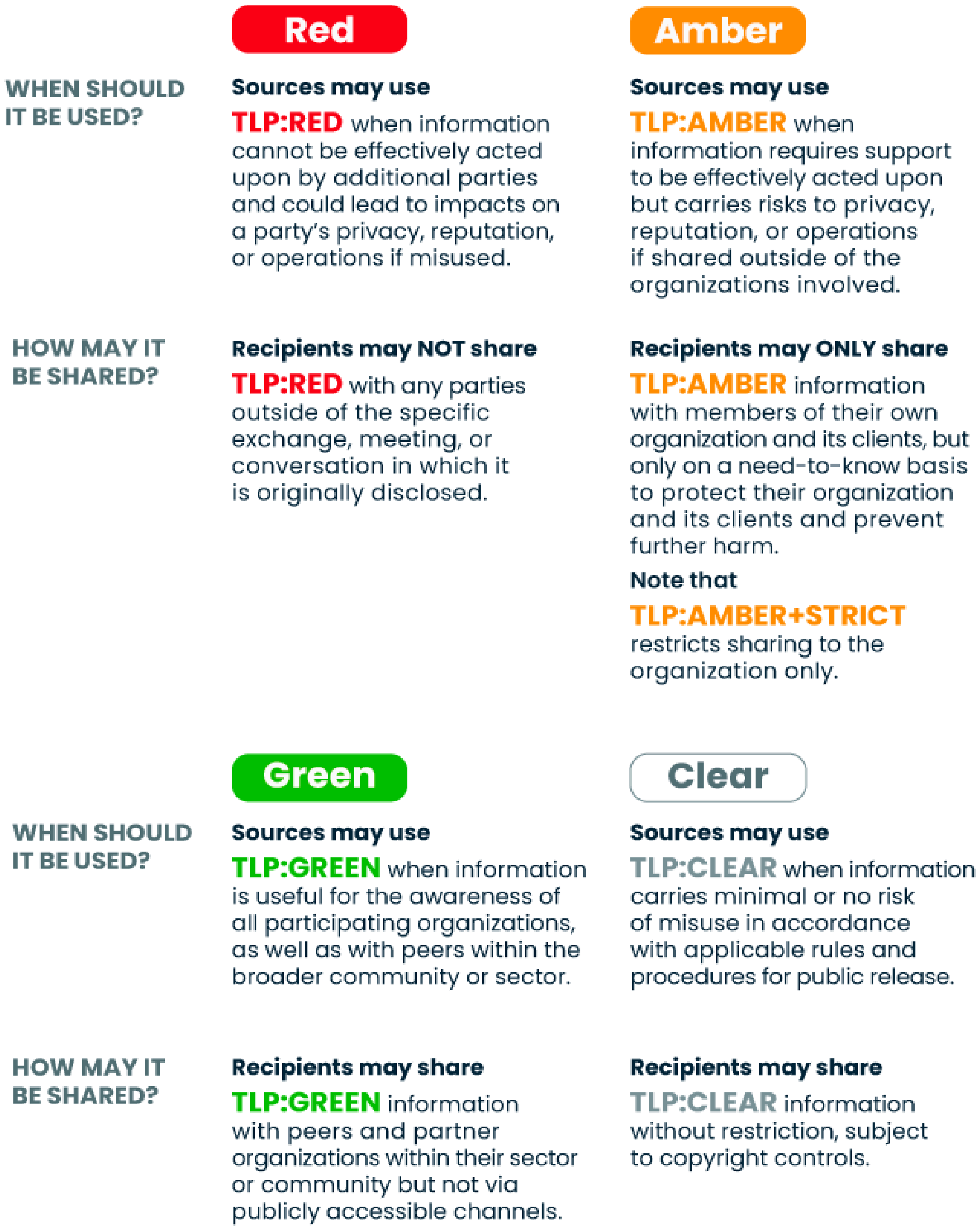
The re-emergence of DanaBot indicates that disrupted cybercrime networks are very likely to reorganize under recognizable branding to reignite their criminal enterprises as long as financial incentives persist. Further, this suggests that Operation Endgame, while significant for its scope and success, was only a limited and temporary disruption of the wider cybercriminal ecosystem. With the launch of DanaBot version 669, law enforcement agencies involved in Operation Endgame are likely to renew their efforts to disrupt this evolving cybercrime threat.

[3] hXXps://www.scworld[.]com/brief/updated-danabot-malware-emerges-after-takedown

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

Appendix A: Traffic Light Protocol for Information Dissemination

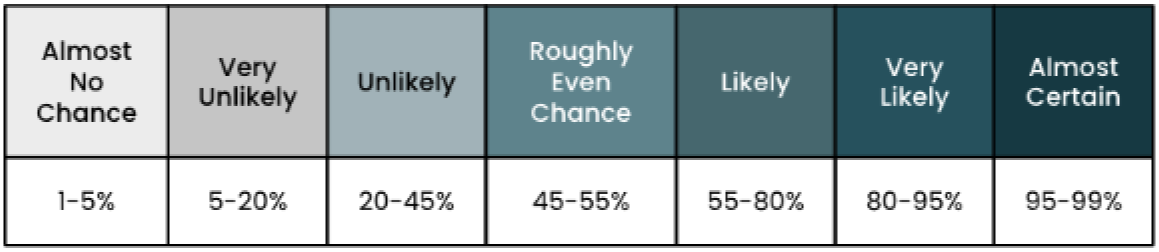


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** **TLP:RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** **TLP:AMBER** information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** **TLP:AMBER+STRICT** restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** **TLP:CLEAR** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** **TLP:GREEN** information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** **TLP:CLEAR** information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.



Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%