Cyber Threat Advisory

June 15, 2023

ZEROFOX

KillNet Claims Imminent Attack on Western Financial Systems

- On June 14, 2023, the pro-Russian hacktivist collective known as KillNet warned in its Telegram channel of an impending powerful attack on the Western financial system in the next 48 hours. The alleged targets include the SWIFT wire transfer system, European, U.S. Banks, and the U.S. Federal Reserve. No other specific entities were named directly in the post outside of SWIFT and the U.S. Federal Reserve. The post claims that threat actors from KillNet, REvil, and Anonymous Sudan will unite for the campaign. Killnet indicates that attack is motivated by the U.S. providing weapons to aid Ukraine stating:

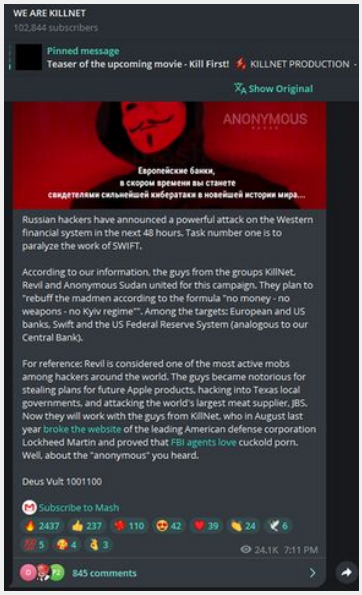
  "repel the maniacs according to the formula" no money – no weapons – no Kiev regime"

- Killnet is known for its politically-motivated targeting (typically Distributed Denial-of-Service (DDoS) attacks) against government agencies, critical infrastructure, and financial institutions across Europe and the United States. While the attacks receive significant media attention, they typically have limited impact, causing short service outages and disrupting access to information.

- Killnet claimed that they would break from their traditional DDoS tactics for this attack; a possible indication of additional capabilities as part of their newly announced partnerships. On June 15, 2023, a Telegram channel "REvil" was created and shared the note "Hello Killnet" that was heavily circulated in a Killnet-affiliated Telegram channel, adding credibility to the partnership. However, this is the only post in channel to date and no additional evidence substantiating the partnership has been observed. If Killnet has partnered with the Ransomware-as-a-service group, REvil, that in 2021 successfully targeted high profile entities including JBS and Kaseya, this would allow them greater access to vulnerability exploitation, network intrusion, and data exfiltration.

- **ZeroFox Intelligence assesses that the attack, if legitimate, is unlikely to result in mass or prolonged outages to Western banking infrastructure, despite the newly claimed relationships with REvil and Anonymous Sudan. Killnet's attacks have had greater–but not long standing–impact against targets such as against U.S. Azure-based healthcare apps. In a similar vein, Anonymous Sudan has primarily relied upon DDoS activity resulting in limited operational impact to targets, despite recently announcing them ahead of time, such as against Microsoft Azure infrastructure.**

- **Despite Killnet advertising attacks prior to committing them, ZeroFox Intelligence cannot rule out that this could be an attempt to generate notoriety around the groups as well as to elicit a reaction from Western governments and financial institutions.**



Source: ZeroFox Intelligence

Recommendations

- Subscribe to ZeroFox Advanced Dark Web Intelligence for updates on new KillNet developments.
- Configure the ZeroFox Intelligence Platform to monitor for current mentions of your organization on KillNet's Telegram channels.
- Beware of spikes in traffic, suspicious emails, and/or unauthorized access to the active directory.

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 12:00 AM (EDT) on June 15, 2023; per cyber hygiene best practices, caution is advised when clicking on any third-party links.