LevelBlue/Labs

Threat Intelligence Newsletter

Welcome to the July edition of the LevelBlue Labs Threat Intelligence newsletter!

LevelBlue Labs is the threat intelligence unit of LevelBlue. LevelBlue Labs includes a global team of threat researchers and data scientists who, combined with proprietary technology in analytics and machine learning (ML), analyze one of the largest and most diverse collections of threat data in the world. Our research team delivers tactical threat intelligence that powers resilient threat detection and response — even as technology evolves, and adversaries change their tactics, techniques, and procedures.

In the Threat Intelligence Newsletter, you will find the most important threat news from the last month, recent updates to USM Anywhere detections, new pulses in OTX, and more.

Latest Threat Intelligence News

SquidLoader: Highly Evasive, New Loader Targeting Chinese Organizations

LevelBlue Labs recently discovered a new highly evasive loader that is being delivered to specific targets through phishing attachments. Due to the lack of previous samples observed in the wild, LevelBlue Labs has named this malware “SquidLoader,” given its clear efforts at decoy and evasion. LevelBlue Labs first observed SquidLoader in campaigns in late April 2024, and predicts it had been active for at least a month prior.

The second-stage payload malware that SquidLoader delivered was a Cobalt Strike beacon, which had been modified to harden it against static analysis. Based on SquidLoader’s configuration, LevelBlue Labs has assessed that the same unknown actor has been observed delivering sporadic campaigns during the last two years, mainly targeting Chinese-speaking victims. Despite studying a threat actor who seems to focus on a specific country, their techniques and tactics may be replicated, possibly against non-Chinese speaking organizations in the near future by other actors or malware creators who try to avoid detections. Link to the blog: https://cybersecurity.att.com/blogs/labs-research/highly-evasive-squidloader-targets-chinese-organizations

Polyfill supply chain attack

A supply chain attack on the Polyfill.io JavaScript service, acquired by a Chinese company earlier this year, has impacted over 100,000 websites. Polyfill was used by web developers to offer support to older browsers. According to Sansec in their report, the new project owner was injecting malicious JavaScript code that redirected visitors to scam and malicious sites without website owners' knowledge.

Since the anounce of the attack by Sansec, they have received DdoS attacks to potentially silent their publication. Google, Cloudfare, Fastly and Namecheap have taken actions to annul the attack and access to the redirected pages.

Authentication Bypass in MoveIT

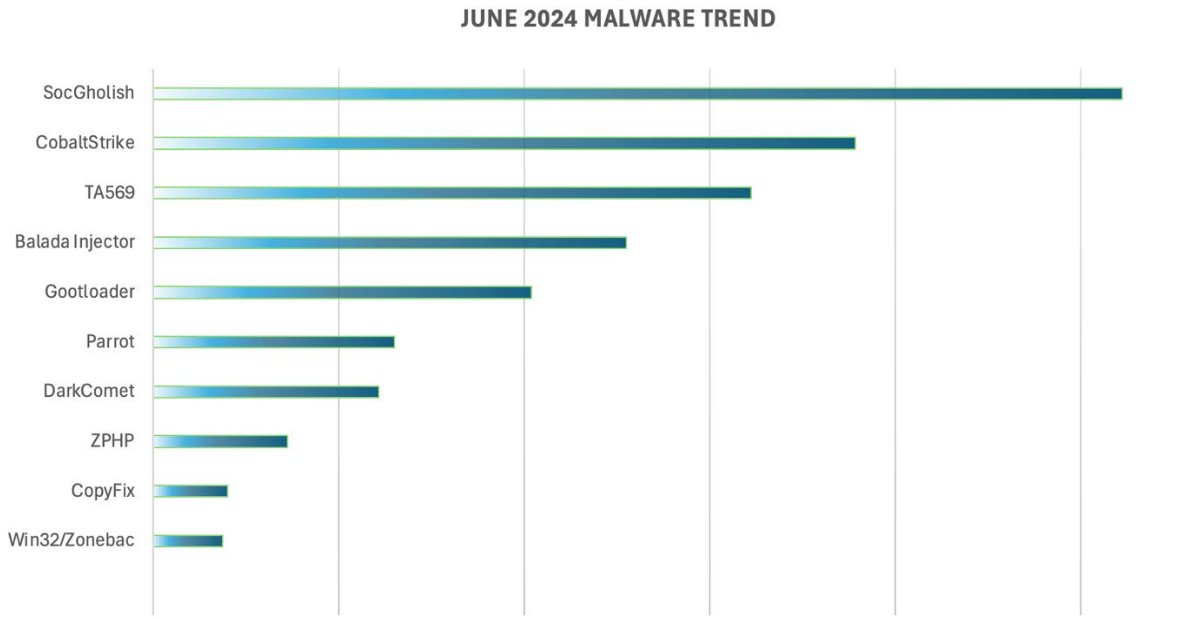
A high-severity authentication bypass vulnerability (CVE-2024-5806) was published on late June for the file sharing platform, MoveIT. The vulnerability allows to inject public keys into the servers and later use them to authenticate with any existing username, impersonating any user with just knowing the username. According to a note from ShadowServer Foundation, there are at least 1,800 exposed instances, but an undertermined number of them being vulnerable.

LevelBlue Labs has not identified active exploits in the wild outside of a handful of IPs scanning systems on mid-June when the vulnerability/exploit had not yet being announced.

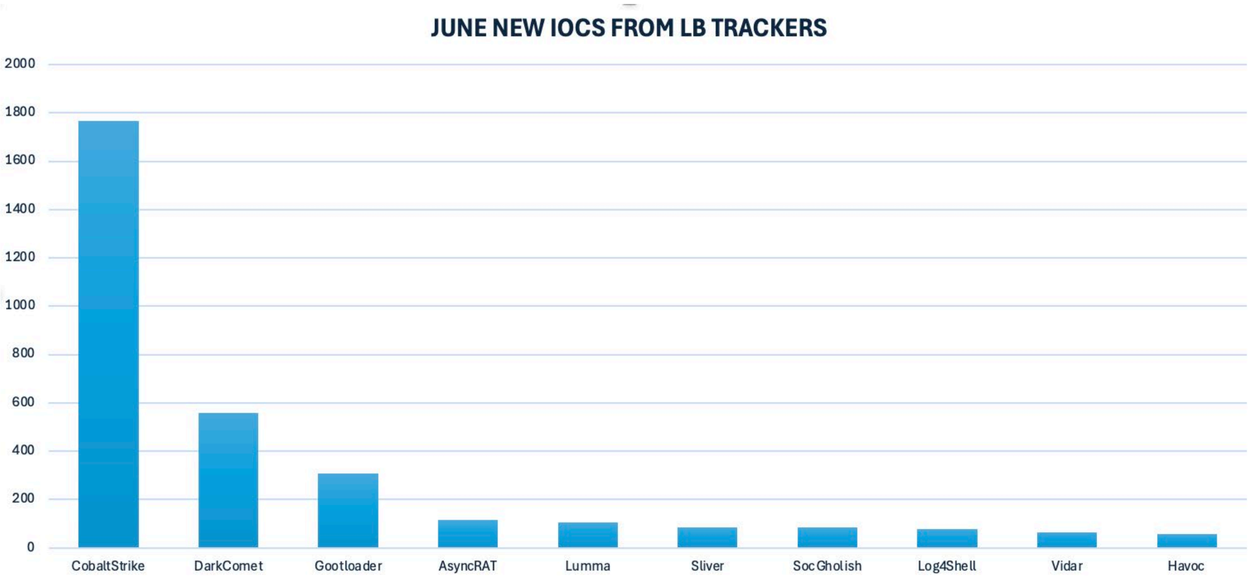
Tracking, Detection & Hunting Capabilities

The team has identified the following malware/threat actors as the most active during the month of June. This month's malware trends continue to be very similar to previous months, with a specially noisy month for:

- **SocGholish**: During the last month, SocGholish indicators have been present in a significant number of investigations, with recently created domains redirecting to the malicious C&C. On top of that, 85 new IOCs were associated with its infrastructure and added to the Threat Intel Tracker.



The LevelBlue trackers have identified over 3700 new IOCs for the different families it tracks. The busiest trackers during the month of June have been:



USM Anywhere Detection Improvements

In June, 112 USM Anywhere detections were added or improved. Here are a few examples of improvements and new elements created:

- Created several new rules related to Anomalous User Behavior for Microsoft Azure, O365 and more.
- Improved Brute Force Authentication rules for repeated login failure for several different technologies, including O365 and Duo.
- Enhanced detections for Active Directory enumerators like SOAPHound and SharpHound.

Please visit the LevelBlue Success Center for a full list of improvements, new elements, issues found, and tasks created.

LevelBlue Labs Open Threat Exchange

LevelBlue Labs Open Threat Exchange (OTX) is the world's largest open threat intelligence community, made up of 450K threat researchers who publish threat information from 140 different countries on the OTX platform, which our LevelBlue Labs team enriches and consumes. You can go here to find out more about the new pulses or to sign up to be part of the community.

New OTX Pulses

The LevelBlue Labs team is continuously creating new Pulses in OTX based on what they are seeing in the wild. In June, 90 new Pulses were created by the Labs team, providing coverage for the latest threats and campaigns. Here are a few examples of the most relevant new Pulses:

- Poseidon Mac stealer distributed via Google ads
- Polyfill supply chain attack hits 100K+ sites
- StrelaStealer Resurgence: Tracking a JavaScript-Driven Credential Stealer Targeting Europe
- Unveiling SpiceRAT: Latest tool targeting EMEA and Asia
- Highly evasive SquidLoader targets Chinese organizations
- SolarMarker Impersonates Job Employment Website
- Arid Viper poisons Android apps with AridSpy
- UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion

- IcedID Brings ScreenConnect and CSharp Streamer to ALPHV Ransomware Deployment

Need More Information?

To have Release Notes emailed to you automatically, follow these steps:

1. Log in to the LevelBlue Success Center.
2. Click on the announcement for the product you wish to follow.
3. Select the “Follow” button on the right-hand side.
4. Select the drop-down menu on the right-hand side and choose “Every Post” to enable receiving emails from leading security and IT tools.