New Evasive SquidLoader Malware Targeting Chinese Organizations

Date: 21th June 2024 | Severity: High

Summary

Cybersecurity researchers have uncovered a new evasive malware loader named SquidLoader that spreads via phishing campaigns targeting Chinese organizations. AT&T LevelBlue Labs, which first observed the malware in late April 2024, said it incorporates features that are designed to thwart static and dynamic analysis and ultimately evade detection. The cybersecurity company said it observed nearly 5,000 distinct victims spread across 10 different campaigns, with a majority of the victims located in the U.S., the U.K., the Netherlands, Poland, France, Czechia, Japan, Australia, Germany, and Canada.

Attack Vectors

- Some of the defensive evasion techniques adopted by SquidLoader encompass the use of encrypted code segments, pointless code that remains unused, Control Flow Graph (CFG) obfuscation, debugger detection, and performing direct syscalls instead of calling Windows NT APIs.
- Loader malware has become a popular commodity in the criminal underground for threat actors looking to deliver and launch additional payloads to compromised hosts, while bypassing antivirus defenses and other security measures.
- The malware employs advanced anti-analysis techniques to evade detection and harden analysis, including system checks, indirect syscalls, encryption of next-stage and strings, and dynamic API resolution.

Indicator of compromise

INDICATOR TYPE	INDICATORS	
IP address	• 101[.]200.228.27 • 107[.]173.248.41 • 112[.]126.85.225 • 122[.]51.216.39	• 182[.]92.123.99 • 39[.]105.204.46 • 47[.]94.227.173 • 82[.]156.184.108

File Hashes	• 597b7e9962b42c4568492aaa44c7164fbf2c1a81d627bc2262a82b05b1e19534 • 01c5b2be71a64b6bbd2029a774f63ed8afc0d122e269e2340c9ab5ec9303318e • 41523349ade62c5d2e9a3274043970ea43ce7c7e5fb2153497979f4b4df1479b • 6d41e0e197b9635f27252dba94293ad714eadcfc39d1627288cb88900ef6e3af • 914b1b3180e7ec1980d0bafe6fa36daade752bb26aec572399d2f59436eaa635 • d81dc8d657477014a3d2a5fdeb507b0573e35f7484e8d0a57eb030211ad89505 • 23a041fd6c1f9ac20bc189f3c74e3ad96a2353c0ac3b917b27966497f40d4d85 • 565fc225391c1d37c15eb8f852819902d801092fdd93eb1da596a97b42ccef0c • 2cd9936fbdd2b98d1abfe9396341501223d35aa43b88a8ca1337dca36f4553ed • 47bdd9282889be2bcf0c70bf52c2da7730a39c4f5a56d93d17793c91381f0db0

Recommendation

1 Implement Strong Security Measures:

- Use Antivirus and Antimalware Solutions: Ensure all systems have up-to-date antivirus and antimalware software installed.
- Regular Software Updates: Keep all software, including operating systems and applications, updated to patch vulnerabilities.
- Firewalls and Intrusion Detection Systems (IDS): Deploy robust firewalls and IDS to monitor and block malicious activities.

2 User Awareness and Training:

- Phishing Awareness: Educate users on recognizing and avoiding phishing emails, which are a common vector for malware distribution.
- Regular Training: Conduct regular security training sessions for employees to keep them informed about the latest threats and safe practices.

3 Network Segmentation

- Limit Access: Segregate critical systems from less sensitive ones to contain any potential malware spread.
- Least Privilege Principle: Implement least privilege access controls to minimize the number of users with administrative privileges.

4 Backup and Recovery

- Regular Backups: Regularly back up critical data and ensure backups are stored securely and tested for integrity.
- Disaster Recovery Plan: Develop and maintain a disaster recovery plan to quickly restore systems in case of an attack.

Reference Links

- https://thehackernews.com/2024/06/experts-uncover-new-evasive-squidloader.html
- https://otx.alienvault.com/pulse/665ecd69888be6a03ec006c3