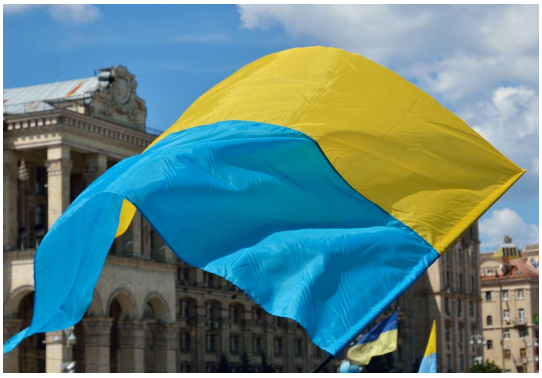
← Go to listing page

GoMet Backdoor Used in Attacks Targeting Ukraine

Breaches and Incidents July 27, 2022 Cyware Alerts - Hacker News



An uncommon malware has been used in an attack aimed at a large Ukrainian software development company. Researchers believe that the attack has been carried out by Russian state-sponsored actors.

What's GoMet backdoor?

GoMet is a simple piece of software written in the Go programming language and includes nearly all the usual functions an attacker prefers in a remotely controlled agent.

- The backdoor supports job scheduling using Cron or task scheduler based on the OS, file download, single command execution, and ability to open a shell or upload a file.
- GoMet features daisy-chain attack ability, whereby attackers gain access to a network or machine to gain access to multiple networks and computers for connections from one infected host to another, thus reaching hosts that are isolated from the internet.

Understanding the campaign

Researchers from Cisco Talos discovered a modified GoMet backdoor being used in attacks targeting a Ukrainian software firm. They believe that it is an attempt to perform supply chain attacks.

- Two samples of the backdoor with minor differences have been discovered, believed to have the same source code.
- In the modified version, the cronjob was set up to run every two seconds instead of every hour. It prevents an hour-long sleep if a connection fails.
- If the malware failed to reach the C2, the backdoor sleeps for a random amount of time between five and ten minutes.
- To prevent forensic analysis, the backdoor enumerats autorun values. Instead of creating new values, it replaced one of the existing goodware autorun executables with the malicious one.

However, whether the attack was successful is not clear.

Ending notes

Ukraine continues to face a series of attacks, GoMet backdoor is among the latest. For staying secure, private and government firms are suggested to stay vigilant and follow the recommendations of CERT-UA. Further, apply the suggested mitigations by the security firms.

GoMet Backdoor | Ukraine | cronjob | Supply Chain Attack

Publisher
Cyware


← PREVIOUS
Chrome Zero-day Abused to Spread Spyware to Target Jour ...
Malware and Vulnerabilities


→ NEXT
Google Ads Abused in Windows Support Scams
Identity Theft, Fraud, Scams

CATEGORIES

- Expert Blogs and Opinion
- Innovation and Research
- The Hacker Tools
- Incident Response, Learnings
- Malware and Vulnerabilities
- Breaches and Incidents
- Laws, Policy, Regulations
- Companies to Watch
- Strategy and Planning
- Mobile Security
- Govt., Critical Infrastructure
- Identity Theft, Fraud, Scams
- Security Culture
- Trends, Reports, Analysis
- New Cyber Technologies
- Major Events
- Cyber Glossary
- Threat Actors
- Security Products & Services
- Threat Intel & Info Sharing
- Emerging Threats
- Geopolitical, Terrorism
- Internet-of-Things
- Computer, Internet Security
- Social Media Threats
- Security Tips and Advice
- Interesting Tweets
- Marketplace
- Did You Know?
- Physical Security

RESOURCES

- Cyber Fusion Center Guide

EVENTS

- Conference
- Webinar
- Summit
- Course
- Symposium
- Talk
- Seminar
- Others

News and Updates, Hacker News

Get in touch with us now!

1-855-692-9927

CYWARE SOCIAL

Download Cyware Social App

Terms of Use Privacy Policy