MUST READ Daixin Team targets health organizations with ransomware, US agencies

Threat actors target software firm in Ukraine using GoMet backdoor

July 21, 2022 By Pierluigi Paganini

Threat actors targeted a large software development company in Ukraine using the GoMet backdoor.

Researchers from Cisco Talos discovered an uncommon piece of malware that was employed in an attack against a large Ukrainian software development company.

The software development company produces software that is used by various state organizations in Ukraine.

Talos researchers pointed out that there are only two documented cases of usage of this backdoor by advanced threat actors. The first one took place in 2020, threat actors were dropping this backdoor after the compromise of a network by exploiting the CVE-2020-5902 vulnerability in F5 BIG-IP. The second time the backdoor was involved took place recently, the attackers deployed the malware after successful exploitation of the CVE-2022-1040 vulnerability in Sophos Firewall.

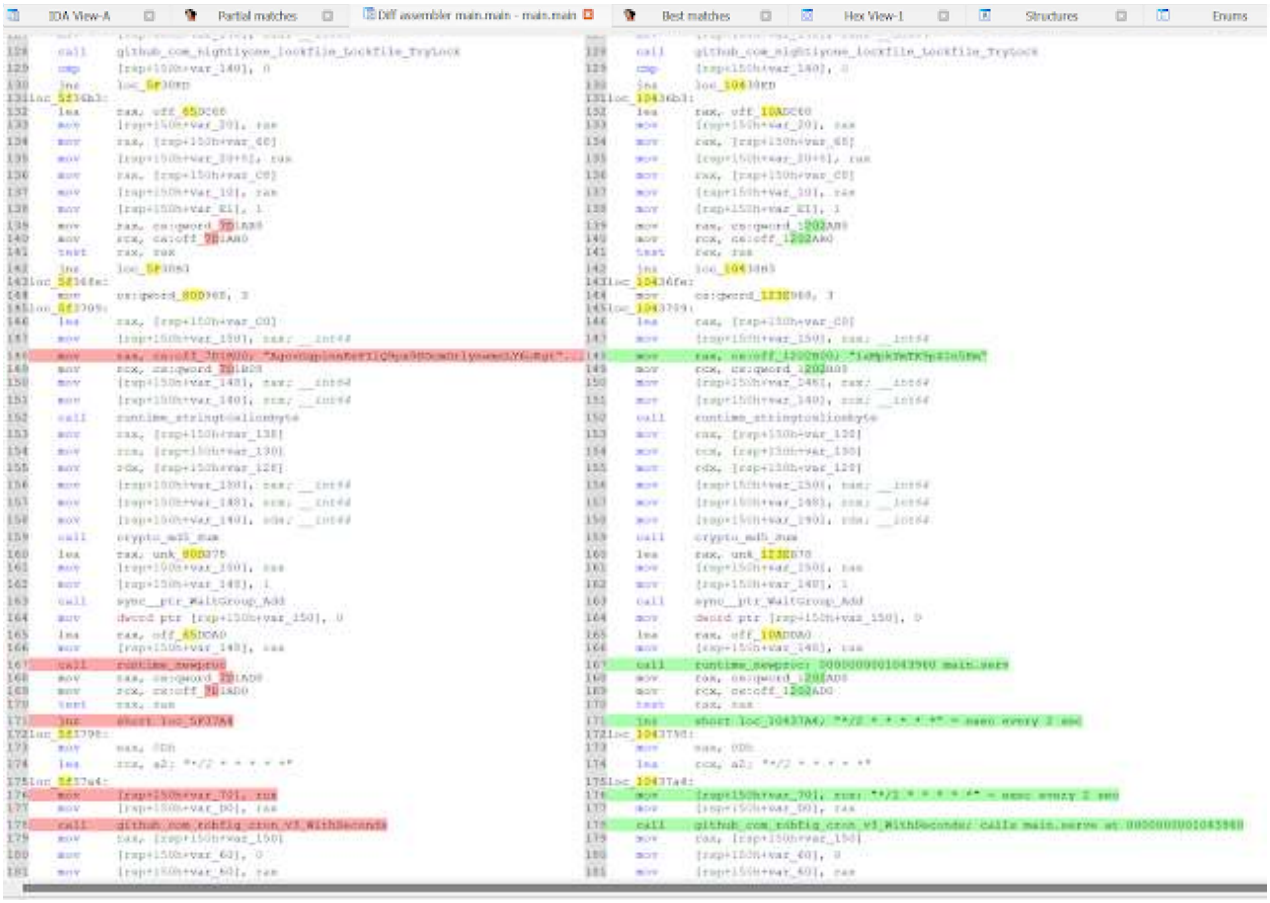
The original GoMet was published on GitHub on March 31, 2019, it had commits until April 2, 2019, but the author has not added any features since its first appearance.

"The backdoor itself is a rather simple piece of software written in the Go programming language. It contains nearly all the usual functions an attacker might want in a remotely controlled agent. Agents can be deployed on a variety of operating systems (OS) or architectures (amd64, arm, etc.). GoMet supports job scheduling (via Cron or task scheduler depending on the OS), single command execution, file download, file upload or opening a shell." reads the analysis published by Talos. "An additional notable feature of GoMet lies in its ability to daisy chain — whereby the attackers gain access to a network or machine and then use that same information to gain access to multiple networks and computers — connections from one implanted host to another. Such a feature could allow for communication out to the internet from otherwise completely "isolated" hosts."

The researchers noticed that the version employed in the attack was changed by the attackers, in particular, the cronjob was configured to run every two seconds instead of every hour. The change prevents an hour-long sleep if the connection fails.

Another change is related to the action that the malware does in case C2 is unreachable, it will sleep for a random amount of time between five and 10 minutes.

Talos researchers found two samples of this backdoor that have minor differences, but that likely use the same source code.



“The malicious activity we detected included a fake Windows update scheduled tasks created by the GoMet dropper. Additionally, the malware used a somewhat novel approach to persistence. It enumerated the autorun values and, instead of creating a new one, replaced one of the existing goodware autorun executables with the malware. This potentially could avoid detection or hinder forensic analysis.” continues the report.

The samples detected by Talos have the IP address of the C2 hardcoded (111.90.139[.]122) and contact it via HTTPS on the default port.

The server uses a self-signed certificate that was issued on April 4, 2021.

“In this instance, we saw a software company targeted with a backdoor designed for additional persistent access. We also observed the threat actor take active steps to prevent detection of their tooling by obfuscating samples and utilizing novel persistence techniques. This access could be leveraged in a variety of ways, including deeper access or launching additional attacks, including the potential for software supply chain compromise.” concludes the report. “It’s a reminder that although the cyber activities haven’t necessarily risen to the level many have expected, Ukraine is still facing a well-funded, determined adversary that can inflict damage in a variety of ways — this is just the latest

(SecurityAffairs – hacking, Ukraine)

Pierluigi Paganini

Pierluigi Paganini is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group and Cyber G7 Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE
Lightning Framework, a previously undetected malware that targets Linux systems

NEXT ARTICLE
TA4563 group leverages EvilNum malware to target European financial and investment entities

YOU MIGHT ALSO LIKE

October 23, 2022 By Pierluigi Paganini

October 23, 2022 By Pierluigi Paganini