Ukraine suffers from another set of backdoor dubbed GoMet

July 29, 2022 By iZOOlogic In Europe

CATEGORIES

- Telecommunications (68)

This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media.

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

To find out more about the cookies we use, see our Privacy Policy.

Accept Decline

firms. Cybersecurity researchers firmly believe that these new attacks came from Russia and were executed by its state-sponsored threat groups.

GoMet is a standard piece of software coded in the Go programming language (Golang) and includes all the usual functions that a threat actor would want in a remotely controlled kit.

In addition, GoMet supports job scheduling tools by utilising Cron, or task scheduler, depending on the operating system (OS), single command execution, and the ability to access a shell or upload a file.

The newly discovered backdoor sports a daisy-chain attack capability in which hackers acquire initial access to a network or device to infiltrate other networks. This ability can also allow the adversaries to secure their connections to other computers from one infected host to another. Hence, threat actors can easily reach hosts isolated from the internet.

- Gaming (62)
- Europe (346)
- Dark Web (118)
- North America (162)
- Fraud Prevention (264)
- South America (145)
- Hacking (390)
- Africa (105)
- Financial Malware (500)
- Middle East (194)
- Phishing (296)
- Central Asia (134)
- SMiShing (14)
- Russia (76)
- Social Media (74)

This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media.

If you decline, your information won’t be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

To find out more about the cookies we use, see our Privacy Policy.

Accept Decline

chain attacks against the country. A few samples of the backdoor were also found with minimal differences, and they believed that despite their differences, they still have similar source codes.

In the altered version of the backdoor, cronjob was set to operate every couple of seconds instead of every hour. The threat actors employ this mechanism to prevent an hour-long sleep if a connection declines.

Additionally, if the malware fails to contact its command-and-control server, it will sleep for a random time, between five to ten minutes. The backdoor will then enumerate autorun values to avoid being examined by forensic analysis.

It also replaces one default goodware autorun executable with the malicious one instead of developing newer values. However, researchers are still puzzled about whether their attacks were successful.

As of now, Ukraine still suffers from the series of attacks which Russia deployed. To stay protected, government and private organisations should remain vigilant and follow the guidelines

- Threat Intelligence (162)
- Digital Risk Protection (282)
- Policy Enforcement (95)
- Risk and Compliance (81)
- Compromised Data (142)
- Domain Names (30)
- Data Breach (135)
- Brand Abuse (93)
- Pharming (5)
- Executive Monitoring (20)
- Website Protection (57)
- Third Party Risk Assessment (116)
- Cryptocurrency (109)

This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media.

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

To find out more about the cookies we use, see our Privacy Policy.

Accept Decline

About the author

iZOOlogic

← PREV NEXT →

Leave a Reply

Comment*

This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media.

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

To find out more about the cookies we use, see our Privacy Policy.

Accept Decline

POST COMMENT

Contact Us

HQ/EMEA

Level 30, The Leadenhall Building 122 Leadenhall Street, EC3V 4AB City of London, UNITED KINGDOM +44 20 3734 2726 info@izoologic.com

Americas

APAC

Global Security Operation Centre

Company

- Our Company
- Corporate Compliance
- Media Enquires

This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media.

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

To find out more about the cookies we use, see our Privacy Policy.

Accept Decline

- Industry News
- Newsletter
- Case Studies
- White Papers
- Technical Datasheets
- iZOOlabs

Copyright © 2020 iZOOlogic, All Right Reserved

This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media.

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

To find out more about the cookies we use, see our Privacy Policy.

Accept Decline