DARKREADING

NEWSLETTER SIGN-UP

VULNERABILITIES & THREATS

APT41 Taps Google Red-Teaming Tool in Targeted Info-Stealing Attacks

China-linked APT41 group targeted a Taiwanese media organization and an Italian job agency with standard, open source penetration test tools, in a change in strategy.

Dan Raywood, Senior Editor, Dark Reading
April 19, 2023

4 Min Read

SOURCE: PIXELS HUNTER VIA SHUTTERSTOCK

The advanced persistent threat known as APT41 has pressed into service an open source, red-teaming tool, Google Command and Control (GC2), for use in cyber espionage attacks marking a shift in its tactics.

According to the Google Threat Analysis Group (TAG) team, the APT41 group, also known as HOODOO, Winnti, and Bronze Atlas, recently targeted a Taiwanese media organization with phishing emails which contained links to a password protected file hosted in Drive.

When the file was opened, it fetched the GC2 payload. As detailed in the TAG April Threat Horizons report, this tool gets its commands from Google Sheets, most likely to hide the malicious activity, and exfiltrates data to Google Drive. The GC2 tool also enables the attacker to download additional files from Drive on to the victim's system.

APT41 also previously used GC2 last July to target an Italian job search website, according to TAG.

TAG researchers noted that incidents such as this highlight several trends by China-affiliated threat actors, such as using publicly available tooling, the proliferation of tools written in the Go programming language, and the targeting of Taiwanese media.

Chinese APT groups have increasingly used publicly available (and legitimate) tools such as Cobalt Strike and other penetration testing software, which is available on sites like GitHub; there's also been a shift to using lesser-known red teaming tools such as Brute Ratel and Sliver to evade detection during their attacks.

The use of such "living off the land" tactics is well known in financially motivated cyberattackers, but less so among APTs that are better resourced and can develop custom tools. Yet Christopher Porter, head of threat intelligence for Google Cloud, said in the report that it is "only prudent to consider that state-sponsored cyber threat actors may steal from the playbooks of cybercriminals to target such systems."

He adds, "A familiar domain name disarms many of the natural defenses we all have when viewing a suspicious email, and the degree to which it is trusted will often be hard coded into security systems screening for spam or malware," he says. He also flagged the use of cloud services for stealth and legitimacy: "Cloud providers are useful targets for these kinds of operations, either as hosts for malware or providing the infrastructure for command-and-control."

Who Is APT41?

The group's activities illustrate the "continued overlap of public sector threat actors targeting private sector organizations with limited government ties," according to the TAG analysis.

Last year the same group was discovered deploying the Spyder Loader malware as part of an ongoing campaign to gather intelligence information on government organizations in Hong Kong, as well as targeting multiple US government agencies using the Log4j vulnerability.

Bronze Atlas is "one of the most prolific groups we have been tracking for a long time," says Marc Burnard, senior security researcher for Secureworks' Counter Threat Unit, having tracked it since at least 2007. And during that time, the group "has been very prolific," he says.

Burnard says APT41 has gone after a range of targets, including government, healthcare, high-tech manufacturing, telcos, aviation, non-governmental organizations (NGOs), and targets in line with China's political and economic interests.

"They are primarily focused on stealing intellectual property, and they have also been involved in targeting political intelligence as well," he notes.

Asked why this particular Taiwanese media company would be targeted, Burnard admits there could be several reasons, including the China-Taiwan political situation, a goal of using the victim to target other organizations and individuals, or there could be a "destructive element" too.

APT41 Quiets Down Its Wall of Noise

As mentioned, the TAG report found that the attackers sent phishing emails to the victim containing links to legitimate cloud services in order to avoid detection — links to a trusted cloud service don't set off email filters. Burnard points out that this is part of a style change for the group, as up until the last few years it was quite noisy in its attacks, and not too worried about the activity being detected.

However, since the 2020 indictment of seven alleged cybercriminals, which reportedly included members of APT41, the activity has been more stealthy and Burnard says the APT is now moving towards using legitimate tools like Cobalt Strike, and towards cloud services, to hide their intent and activity.

About the Author(s)

Dan Raywood, Senior Editor, Dark Reading

With more than 20 years experience of B2B journalism, including 12 years covering cybersecurity, Dan Raywood brings a wealth of experience and information security knowledge to the table. He has covered everything from the rise of APTs, nation-state hackers, and hacktivists, to data breaches and the increase in government regulation to better protect citizens and hold businesses to account. Dan is based in the U.K., and when not working,...

You May Also Like

Vulnerabilities & Threats ganization Launches Pen-Testing Training Group

Vulnerabilities & Threats e Issues Major Security Advisory

Vulnerabilities & Threats Exploit Code for Critical Fortinet VPN Bug

Vulnerabilities & Threats s Pose Major Cybersecurity Risk to Enterprises

More Insights

Webinars

What's In Your Cloud?
JAN 17, 2024

Everything You Need to Know About DNS Attacks
JAN 18, 2024

Tips for Managing Cloud Security in a Hybrid Environment
FEB 01, 2024

Top Cloud Security Threats Targeting Enterprises
FEB 08, 2024

DevSecOps: The Smart Way to Shift Left
FEB 14, 2024

More Webinars

Events

Black Hat Asia - April 16-19 - Learn More

Black Hat Spring Trainings - March 12-15 - Learn More

Cyber Resiliency 2023: How to Keep IT Operations Running, No Matter What

More Events

Editor's Choice

IOT

ICS/OT SECURITY

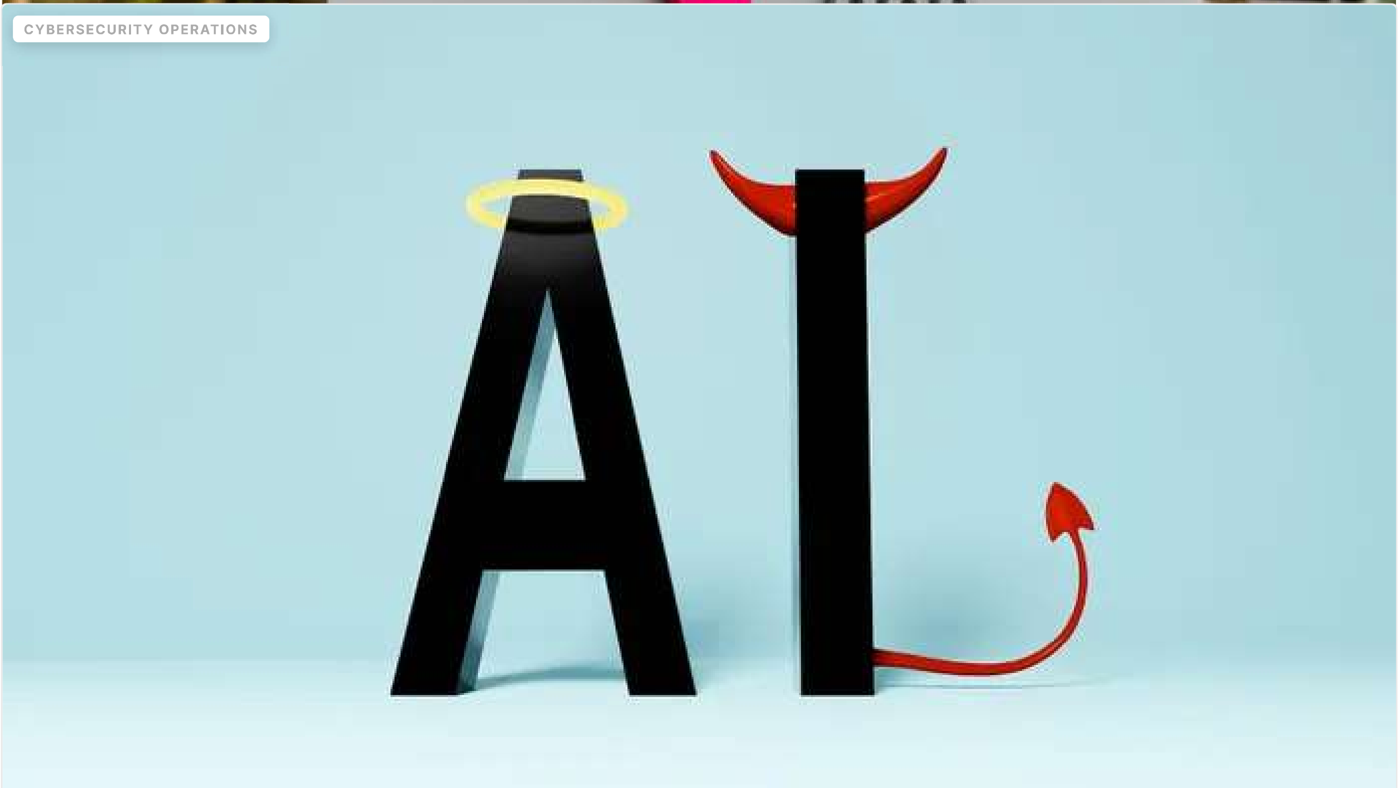
Patch Now: Critical Windows Kerberos Bug Bypasses Microsoft Security

by Jai Vijayan, Contributing Writer

JAN 9, 2024 5 MIN READ

CYBERATTACKS & DATA BREACHES

CYBERSECURITY OPERATIONS



CISO Planning for 2024 May Struggle When It Comes to AI

by **Joan Goodchild, Contributing Writer**

JAN 2, 2024 4 MIN READ

Reports

Passwords Are Passe: Next Gen Authentication Addresses Today's Threats

The State of Supply Chain Threats

How to Deploy Zero Trust for Remote Workforce Security

What Ransomware Groups Look for in Enterprise Victims

How to Use Threat Intelligence to Mitigate Third-Party Risk

More Reports

IT Zero Trust vs. OT Zero Trust: It's all about Availability

Buyer's Guide: Choosing a True DevSecOps Solution for Your Apps on AWS

2023 Software Supply Chain Attack Report

The Need for a Software Bill of Materials

The Developers Guide to API Security

More Whitepapers

Events

Black Hat Asia - April 16-19 - Learn More
APR 16, 2024

Black Hat Spring Trainings - March 12-15 - Learn More
MAR 12, 2024

Cyber Resiliency 2023: How to Keep IT Operations Running, No Matter What
AUG 24, 2023

More Events

DARKREADING

Discover More With Informa Tech

Black Hat

Omdia

Working With Us

About Us

Advertise

Reprints

Join Us

NEWSLETTER SIGN-UP

Follow Us

Home | Cookie Policy | Privacy | Terms of Use

Cookies Preference Center

When you visit any website, it may store or retrieve information on your browser, mostly in the form of cookies. This information might be about you, your preferences or your device and is mostly used to make the site work as you expect it to. The information does not usually directly identify you, but it can give you a more personalized web experience. Because we respect your right to privacy, you can choose not to allow some types of cookies. Click on the different category headings to find out more and change our default settings. However, blocking some types of cookies may impact your experience of the site and the services we are able to offer.

More information

Allow All

Manage Consent Preferences

Strictly Necessary Cookies

Always Active

These cookies are necessary for the website to function and cannot be switched off in our systems. They are usually only set in response to actions made by you which amount to a request for services, such as setting your privacy preferences, logging in or filling in forms. You can set your browser to block or alert you about these cookies, but some parts of the site will not then work. These cookies do not store any personally identifiable information.

Performance Cookies

Always Active

These cookies allow us to count visits and traffic sources so we can measure and improve the performance of our site. They help us to know which pages are the most and least popular and see how visitors move around the site. All information these cookies collect is aggregated and therefore anonymous. If you do not allow these cookies we will not know when you have visited our site, and will not be able to monitor its performance.

Functional Cookies

Always Active

These cookies enable the website to provide enhanced functionality and personalisation. They may be set by us or by third party providers whose services we have added to our pages. If you do not allow these cookies then some or all of these services may not function properly.

Targeting Cookies

Always Active

These cookies may be set through our site by our advertising partners. They may be used by those companies to build a profile of your interests and show you relevant adverts on other sites. They do not store directly personal information, but are based on uniquely identifying your browser and internet device. If you do not allow these cookies, you will experience less targeted advertising.

Back