CYBERATTACKS & DATA BREACHES

Chinese Group Built Advanced Trojan by Reverse Engineering NSA Attack Tool

APT3 quietly monitored an NSA attack on its systems and used the information to build a weapon of its own.

Jai Vijayan, Contributing Writer

September 7, 2019

4 Min Read

Chinese threat actor APT3 quietly monitored the US National Security Agency's use of a highly sophisticated cyber attack tool and then reverse engineered the code to build an advanced Trojan of its own called Bemstour.

That conclusion, by Check Point Software, is based on the security vendor's analysis of Bemstour after Symantec in May reported on APT3 using it in attacks on targets in multiple countries, including Belgium, Hong Kong and the Philippines.

Symantec had described APT3 as using Bemstour to deliver a variant of a backdoor called DoublePulsar on target systems. Symantec said its analysis showed both tools appeared to be variants of attack software built by Equation Group, an operation affiliated with the NSA's Tailored Access Operations unit.

Symantec said it was unclear how APT3 had obtained the NSA tools. But it ruled out the possibility that the Chinese threat actor had obtained the weapons from the large trove of NSA cyber weapons that hacking outfit Shadow Brokers publicly leaked in 2017.

According to Symantec, its analysis showed that APT3 was using Bemstour and DoublePulsar well before the Shadow Brokers data dump. The two variants also had differences in code that made it very clear they did not originate from the leak, Symantec had noted.

Check Point's analysis of Bemstour shows that the exploit is in fact APT3's own implementation of EternalRomance, a tool that the NSA developed to break into Windows 7, Windows 8, and some Windows NT systems, the security vendor said.

APT3 developed the exploit by reverse-engineering EternalRomance, but then tweaked it so it could be used to target more systems. APT3's Bemstour leveraged the same Windows zero-day as the one used in EternalRomance (CVE-2017-0143). In addition the group also created an exploit for another Windows zero-day (CVE-2019-0703). Both flaws have been patched.

"What we found out is that in terms of the software vulnerabilities targeted by the underlying exploit they were identical to those leveraged by EternalRomance," says Mark Lechtik, lead security researcher at Check Point.

"This is no coincidence - finding the exact same set of bugs in order to create an exploit that provides remote code execution capabilities is very unlikely," he says. At the same time, there are enough differences in Bemstour to indicate the exploit was re-engineered and built from scratch, rather than copied wholesale. That is what led Check Point to conclude that an NSA exploit was used in some way as a reference, he notes.

Close Monitoring

During the analysis of Bemstour, Check Point researchers found evidence suggesting the Chinese group had closely monitored systems under its control that the NSA had managed to compromise. APT3 members then captured traffic related to those attacks—including

information on how the NSA was moving laterally on the compromised networks—and then used that as a reference to reverse-engineer the NSA's exploit.

This allowed them to build an exploit tool that looked and worked remarkably similar to the NSA's exploit, but with less effort and cost. Instead of purchasing from a third party or investing in its own in-house team, APT3 built its malware by collecting and using the NSA's own attack data.

"The main takeaway is that we see evidence for the first time of a nation-state collecting and reusing foreign attack tools to recreate their own," Lechtik says. "We heard of that happening in theory; now we [have] facts that support it."

Lechtik says it's unclear if other Chinese APT groups and state actors have adopted a similar approach. But from their point of view, the approach would make sense. "If they can catch a tool and repurpose it, they cut the costs on finding it themselves," he notes. "If we see they did it once, it would be likely they have done it on other instances and keep doing it today."

The question of whether other countries are doing the same thing is harder to answer, he says. Pulling off something like what APT3 did requires the ability to deliberately monitor domestic systems, collect and analyze a lot of information all with the hope of finding one usable tool.

"Not all nation-states would go down this road in the first place, and indeed a lot don't use exploits, not to mention zero-days, almost at all," he says. "Instead, they try to abuse human weaknesses through phishing, for example—an opportunistic but very cheap alternative. Iran and North Korea are examples for exactly that."

Related Content:

- **APT3 Threat Group a Contractor for Chinese Intelligence Agency**
- **Shadow Brokers Offers Database Of Windows Exploits For Sale**
- **The Shadow Brokers: How They Changed 'Cyber Fear'**
- **8 Head-Turning Ransomware Attacks to Hit City Governments**

Check out The Edge, Dark Reading's new section for features, threat data, and in-depth perspectives. Today's top story: "8 Ways To Spot an Insider Threat."

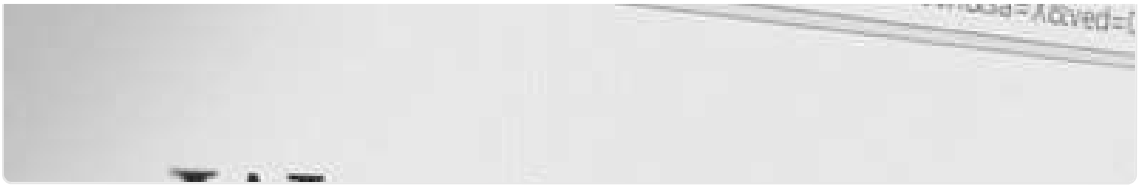
About the Author(s)

Jai Vijayan, Contributing Writer

Jai Vijayan is a seasoned technology reporter with over 20 years of experience in IT trade journalism. He was most recently a Senior Editor at Computerworld, where he covered information security and data privacy issues for the publication. Over the course of his 20-yea...

You May Also Like

Cyberattacks & Data Breaches



Inside Job: Cyber Exec Admits to Hospital Hacks

Iran APT Targets the Mediterranean With Watering-Hole Attacks

Cyberattacks & Data Breaches

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

CES 2024: Will the Coolest New AI Gadgets Protect Your Privacy?

by **Nate Nelson, Contributing Writer**

ICS/OT SECURITY

Patch Now: Critical Windows Kerberos Bug Bypasses Microsoft Security

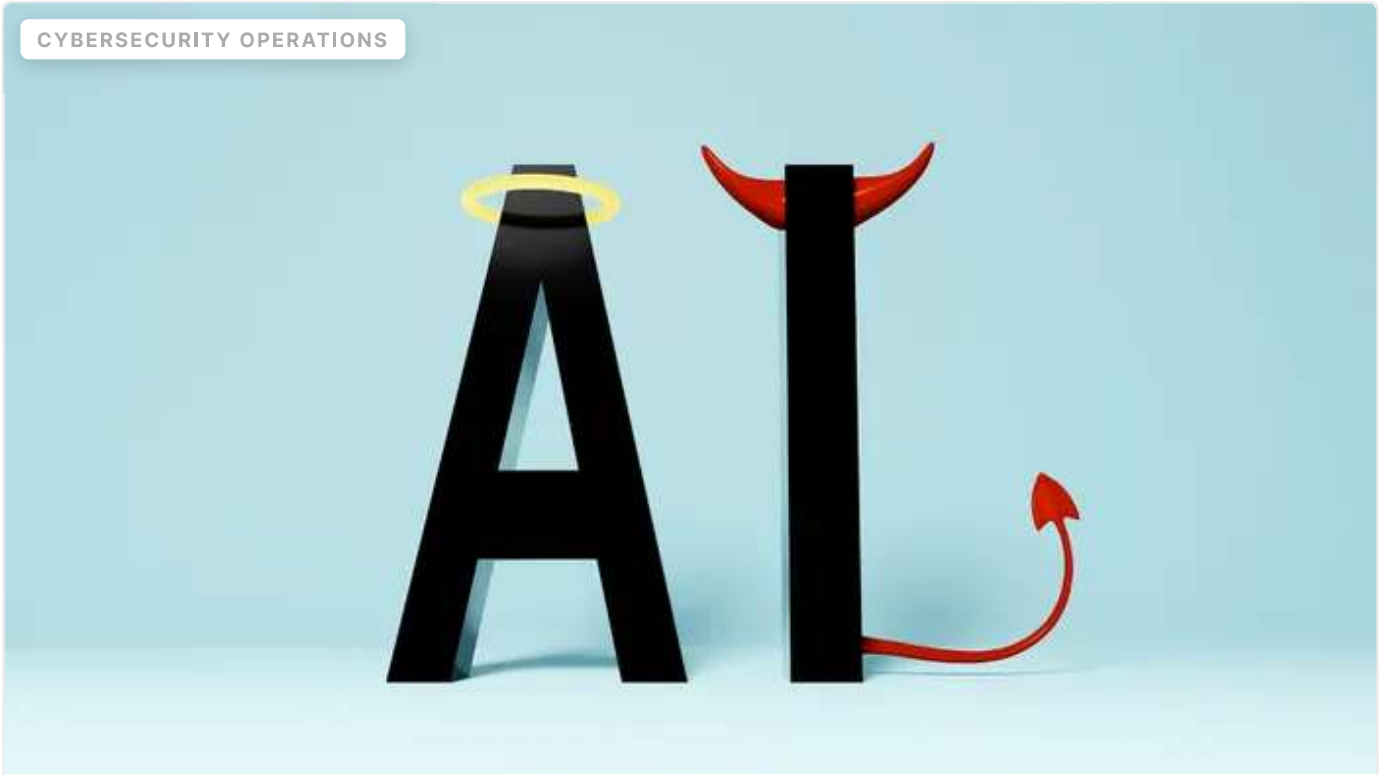
by **Jai Vijayan, Contributing Writer**

JAN 9, 2024 5 MIN READ

CYBERATTACKS & DATA BREACHES

23andMe: 'Negligent' Users at Fault for Breach of 6.9M Records

by **Nate Nelson, Contributing Writer**



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

White Papers

Pixelle's OT Security Triumph with Security Inspection

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

Understanding AI Models to Future-Proof Your AppSec Program

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