← Go to listing page

APT3: A Nation-State Sponsored Adversary Responsible For Multiple High Profile Campaigns

Research and Analysis · Threat Actor

Share Blog Post

Threat Actor Profile

Origin: China, 2010

Aliases: Gothic Panda, Pirpi, UPS Team, Buckeye, Threat Group-0110, TG-0110

Key Target Sectors: Aerospace, Defense, Construction and Engineering, High Tech, Telecommunications, and Transportation

Attack Vectors: Spear Phishing, Backdoor, Zero-day Attacks

Target Region: Eastern Asia, North America

Malware Used: Shotput, Sogu, PlugX, OSInfo, RemoteCMD, DoublePulsar, FuzzBunch, EternalBlue,

Tools Used: Schtasks, CookieCutter

Overview

APT3 (aka Gothic Panda, Pirpi, Buckeye) is a China-based threat group that was first discovered in 2010. The group is linked to the Chinese Ministry of State Security (China's Intelligence Services) and held responsible for several popular cyber espionage campaigns, including Operation Clandestine Wolf (2015), Clandestine Fox (2014), and Double Tap (2014). The group is known to target countries like South Korea, Hong Kong, and the United States of America.

Which organizations have they targeted?

APT3 has targeted organizations in various sectors, including Aerospace, Defense, Transportation, Telecommunications, Construction Engineering, and High Tech. In the initial years of its discovery, the group mostly targeted US-based organizations of strategic importance, like Moody's Analytics, Siemens AG, and Trimble, Inc. In 2015, the group shifted its focus from US victims to political organizations located in Hong Kong (because of upcoming Hong Kong's 2016 elections). In March 2018, the Olympic Winter Games in Pyeongchang, South Korea, was hit by a cyber attack (OlympicDestroyer), that caused temporary disruption to IT systems, including the official Olympics website, Wi-Fi connections and display monitors. The numerous code fragments used in that cyber attack were uniquely linked to threat actor groups tracked as APT3, APT10, and APT12.

What is their motivation behind the attacks?

The threat actors are interested in the exfiltration of essential government documents to gain a strategic and competitive advantage for the Chinese government and private organizations. For instance, at present when several ambitious projects of China are unfolding, like One Belt One Road (OBOR) projects, the APT3 could be seen targeting the project's regional opponents.

Modus Operandi

APT3 has a history of using browser-based exploits such as zero-days (e.g., Adobe Flash Player, Firefox, and Internet Explorer) to infiltrate inside the targeted network. For instance, in one of their cyber campaigns in April 2014 (Operation Clandestine Wolf), they exploited a now-patched vulnerability (CVE-2015-3113) in Adobe Flash Player 18.0.0.161. After successfully exploiting and infiltrating into a targeted host, they quickly dump credentials, move sideways to additional hosts, and install the custom backdoors (like RemoteCMD, OSInfo, and ShotPut). APT3 is also known to use spear-phishing emails with compressed executable attachment. The APT's command and control (CnC) infrastructure is hard to track and attribute, as there is little overlap across their campaigns (as it happened only once when the same domain was used in operation Clandestine Fox and Double Tap).

Known tools and malware

APT3 utilizes a wide range of techniques and tools, including spearphishing attacks, zero-day exploits, as well as custom-built malware. The group also used variants of the sophisticated hacking tools connected to other popular groups, including the Equation Group.

Known Zero Days Vulnerabilities

- **Unicorn Bug (CVE-2014-6332)** - A critical vulnerability that allows remote code execution in

disclosure vulnerability that exists in the way that the Windows SMB Server handles certain requests.

- **Windows SMB Remote Code Execution Vulnerability (CVE-2017-0143)** - A remote code execution vulnerability that exists in the way the Microsoft Server Message Block 1.0 (SMBv1) server handles specific requests. This vulnerability is used in EternalSynergy and EternalRomance exploits.
- **Adobe Flash Player Heap-based buffer overflow (CVE-2015-3113)** - An unspecified heap-based buffer-overflow vulnerability in Adobe Flash Player.
- **Windows Kernel-Mode Vulnerability (CVE-2014-4113)** - An local privilege-escalation vulnerability that existed in Microsoft Windows-based platform.

Note - All the above vulnerabilities have been patched by the respective vendors, and updated versions can be downloaded from their websites.

Malicious programs used by APT3

- **PlugX** - It is a remote access tool (RAT), based on modular plugins. Multiple threat groups have been using it for various campaigns.
- **Sogu** - It is a Trojan horse that opens a back door on the compromised computer.
- **DoublePulsar, FuzzBunch, EternalBlue, EternalSynergy, and EternalRomance** - Sophisticated tools connected to the Equation Group, an NSA-linked APT group. APT3 had used these tools for more than a year before the Shadow Brokers leak happened in Summer 2016.

Known Commercial/Open Source tools used by APT3

- **Schtasks** - It is used to schedule the execution of programs or scripts on a Windows system to run at a specific date and time.
- **CookieCutter** - A command-line utility that creates projects from project templates (E.g. Python package projects, jQuery plugin projects).

an internal discovery on a victim's computer and network.

- **ShotPut -** It is a custom backdoor used by APT3.
- **RemoteCMD -** It is a custom tool used by APT3 to execute commands on a remote system similar to Sys Internal's PSEXEC functionality.

Attribution

In 2016, three individuals responsible for purchasing APT3 domains for cyber-espionage campaigns were identified, named as Wu Yingzhuo, Dong Hao and Xia Lei. All three individuals had a long history of purchasing infrastructure used by APT3. Wu Yingzhuo and Dong were the major shareholders of a Chinese InfoSec company called the Guangzhou Boyu Information Technology Company, Ltd. (Boyusec). The Pentagon intelligence officials identified Boyusec as being a contractor for the Chinese Ministry of State Security (MSS). In Nov 2017, an indictment was unsealed in the USA against them.

Prevention

To thwart off cyber-attacks from threats like APT3, the organizations should deploy endpoint protection solutions with real-time intelligence and automated tactical threat intelligence exchange. Given the prevalence of attacks used by APT3 that exploit known vulnerabilities, rigorous patch management, and vulnerability assessments practices are a must. Combating APTs like this requires a combination of techniques and tools that ideally work in an orchestrated manner. Orchestration tools that allow real-time Threat Intel ingestion, analysis, correlation, dissemination and actioning through automated Playbooks can go a long way in tackling the nefarious designs of such APTs. Network monitoring can also help expose suspicious activities, like using network APT

training to IT professionals and employees with phishing simulations, tough policies and periodic refreshers that discourage unsafe behaviors.

Indicators of Compromise

SHA1

0311CEC923C57A435E735E106517797F
104ECBC2746702FA6ECD4562A867E7FB
12668F8D072E89CF04B9CBCD5A3492E1
19C539FF2C50A0EFD52BB5B93D03665A
221C6DB5B60049E3F1CDBB6212BE7F41
3514205D697005884B3564197A6E4A34
3C0D740347B0362331C882C2DEE96DBF
47E67D1C9382D62370A0D71FECC5368B
4C8FA3731EFD2C5097E903D50079A44D
4F43F03783F9789F804DCF9B9474FA6D
51545ABCF4F196095ED102B0D08DEA7E
52775F24E230C96EA5697BCA79C72C8E
567D379B87A54750914D2F0F6C3B6571
5778D8FF5156DE1F63361BD530E0404D
583F05B4F1724ED2EBFD06DD29064214
58DD6099F8DF7E5509CEE3CB279D74D5
59C3F3F99F44029DE81293B1E7C37ED2
64AA21201BFD88D521FE90D44C7B5DBA
65C024D60AF18FFAB051F97CCDDFAB7F
68970B2CD5430C812BEF5B87C1ADD6EA
6E0EBEEEA1CB00192B074B288A4F9CFE
7C3BF9AB05DD803AC218FC7084C75E96
83D8D40F435521C097D3F6F4D2358C67
86D1A184850859A6A4D1C35982F3C40E

MD5 Hashes

7020bcb347404654e17f6303848b7ec4
aacfef51a4a242f52fbb838c1d063d9b
c2f902f398783922a921df7d46590295
6458806a5071a7c4fefae084791e8c67
0d2d0d8f4989679f7c26b5531096b8b2
a3932533efc04ac3fe89fb5b3d60128a
58f784c7a2921032519303 60f9ca713e

492a839a3bf9c61b7065589a18c5aa8d
744a17a3bc6dbd535f568ef1e87d8b9a
2fab77a3ff40e4f6d9b5b7e813c618e4
F34d5f2d4577ed6d9ceec516c1f5a744
5c08957f05377004376e6a622406f9aa

SHA256 Hashes
951f079031c996c85240831ea1b61507f91990282daae6
da2841311322e8a6d7
1c9f1c7056864b5fdd491d5daa49f920c3388cb8a8e462b
2bc34181cef6c1f9c
3dbe8700ecd27b3dc39643b95b187ccfd44318fc88c5e6e
e6acf3a07cdaf377e
7bfad342ce88de19d090a4cb2ce332022650abd68f34e8
3fdc694f10a4090d65
6b1f8b303956c04e24448b1eec8634bd3fb2784c8a2d12
ecf8588424b36d3cbc
01f53953db8ba580ee606043a482f790082460c8cdbd7ff
151d84e03fdc87e42
53145f374299e673d82d108b133341dc7bee642530b560
118e3cbcdb981ee92c
cbe23daa9d2f8e1f5d59c8336dd5b7d7ba1d5cf3f0d45e6
6107668e80b073ac3

Domains
Inform.bedircati[.]com
Pn.lamb-site[.]com
Securitywap[.]com
Join.playboysplus[.]com
walterclean[.]com

Originating IP Address
210[.]109[.]99[.]64
192[.]184[.]60[.]229
192[.]184[.]60[.]229
104[.]151[.]248[.]173
104[.]151[.]248[.]173
104[.]151[.]248[.]173

TAGS

apt3 plugx gothic panda olympicdestroyer

Posted on: May 28, 2019

PREVIOUS
APT33: The Lesser Known Adversary With T...

NEXT
APT1: A Nation-State Adversary Atta...

Recent Posts

January 09, 2024

Reflecting on the Past Year: Considering its Impact on the F...

In his insightful article, Avkash Kathiriya, Sr. VP – Research and Innovation ...

threat intelligence sase + 7 more

December 22, 2023

Cybersecurity Gets Personal: How Cyware Boosts Customizable ...

When managed security service providers (MSSPs) get personal, it's not abo...

managed security service providers mssps mssp

December 20, 2023

Cost-Effective Cybersecurity: How MSSPs can Maximize ROI wit...

In cybersecurity, Managed Security Service Providers (MSSPs) are increasin...

managed detection and response tip + 4 more

More from Cyware

Stay updated on the security threat landscape and technology innovations at Cyware with our threat intelligence briefings and blogs.

Daily Threat Briefing

Cyware Daily Threat Intelligence, January 15, 2024


Weekly Threat Briefing
Cyware Weekly Threat Intelligence, January 08–12, 2023

Monthly Threat Briefing

Cyware Monthly Threat Intelligence, December 2023

The Virtual Cyber Fusion Suite

CSAP

Collaborate

CTIX

Intel Exchange

CFTR
Respond

Explore Solutions

Capabilities

Resource Library

Use Cases

Products

Cyber Fusion Center

Threat Intelligence Platforms (TIP)

Intel Exchange (CTIX)

Intel Exchange Lite

Collaborate (CSAP)

Security Orchestration and Automation (SOAR)

Respond (CFTR)

Orchestrate

Intel Exchange Spoke

Cyware Browser Extension

Partners

Channel Partners

MSSPs

Technology Alliances

Open APIs

MISP

Register a Deal

CywareOne Login

Resources

Resource Library

Cyware Labs: Research & Threat Briefings

Security Guides

Free Threat Intel Feeds

Webinars & Videos

Community Resources

Cyware Academy

Company

Leadership

Careers We're Hiring

Cyware in the News

Press Releases

Compliance

Contact Us

Learn More

Blog

TIP Replacement

SOAR Replacement

Request a Demo

Support

Legal

Get in touch with us now!

1-855-692-9927