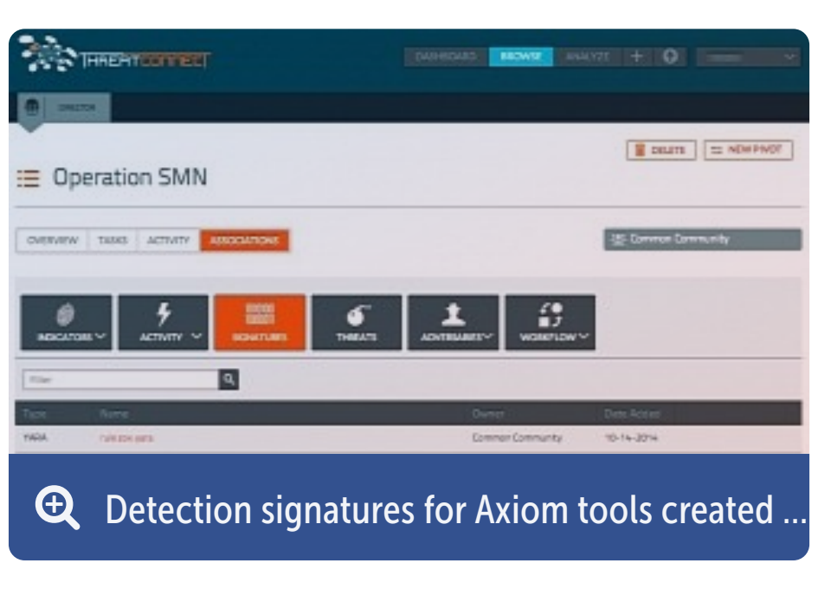
Chinese APT Group Axiom Is Highly Technical and Disciplined

Group exhibits rarely seen level of sophistication

Oct 28, 2014 16:01 GMT · By Ionut Ilascu · Comment · Share:

The Chinese cyber espionage group Axiom, whose activity was detailed on Tuesday, is said to have directed attacks towards a wide set of organizations across the world, also being responsible for resonant cyber incidents in the US that occurred in the past six years.



Detection signatures for Axiom tools created ...

The information about the threat actor has been collected into a common threat intelligence database from multiple private security firms; they gathered into a coordinated action named Operation SMN in order to disrupt the activity of Axiom.

Part of the coalition are Cisco, FireEye, F-Secure, iSIGHT Partners, Microsoft, Tenable, ThreatConnect, ThreatTrack Security, Volexity, Novetta, and Symantec.

Significant attacks linked to Axiom identified since 2009

As a result of this effort, signatures were created for detecting the malicious tools wielded by Axiom, and delivered to partners for protecting their customers, through Microsoft's Virus Information Alliance (VIA), a collaborative security program dedicated to the fight against cybercrime.

From the pool of common intelligence, Operation SMN identified several malicious events that shared similar tactics, techniques and procedures (TTP) with Axiom. These include incidents that go as far back as 2009: Operation Aurora, Elderwood Project, VOHO campaign, Bit9 compromise, Shell Crew, Deputy Dog, Ephemeral Hydra, and Operation Snowman.

According to a report from Novetta, the company leading the Operation SMN campaign, in carrying out these attacks, Axiom relied on a wide set of methods that involved the use of critical zero-day vulnerabilities (either developed in-house or acquired from third parties), leveraging the watering-hole compromise technique or stealing digital certificates, all pointing to a rarely seen level of technical, organizational and operational skills.

Furthermore, some of the tools and infrastructure used for these attacks are the same the ones attributed to the Chinese advanced persistent threat group.

A full compromise follows multiple attack stages

The report reveals that full compromise of a target was achieved through multiple attack stages, which could be performed by other groups associated with Axiom, culminating with the delivery of Hikit rootkit, responsible for data exfiltration.

In the first step, identification of the target and general reconnaissance activity is initiated, followed by the initial access, validation and exploring the internal target.

Additional endeavors refer to expanding to other machines in the network and achieving persistency. The fourth stage supposes identification of the data of interest and exfiltrating it.

A fifth stage ensues, which consists in maintaining access to the target and understanding the environment, for future exploration.

Axiom would manage large numbers of compromised machines and analyze them sometimes in a matter of hours in order to determine the organizations of interest and start the second stage of the attack.

Separate tools are used for each attack stage

The group would leverage the following tools in their effort to compromise a target: Zox family/Gresim, Hikit, Derusbi, Fexel/Deputy Dog, Hydraq/9002/Naid/Roarur/Mdmbot, ZXShell/Sensode, PlugX/Sogu/Kaba/Korplug/DestroyRAT, Gh0st/Moudour/Mydoor and Poison Ivy/Darkmoon/Breut.

Interesting to note is that each attack stage would rely on a different infrastructure and tool set, which was often dictated by the type of the target. Moreover, there would be no connection between the network used in the first level of compromise and the later stages.

This adds to the several evasion techniques used by Axiom, which also involve relying on Hikit binaries customized for each victim and isolating the command and control (C&C) servers for each target.

Operation SMN managed to remove from the computer systems of partners more than 43,000 installations of tools relating to Axiom. In 180 cases, the infection was with Hikit, which translates into the amount of instances of late-stage compromise from Axiom.

“For Stage 3 and 4 operations, Axiom is believed to have established a complex C2 infrastructure, which, based on campaign identifiers extracted from configuration files embedded in Hikit binaries, has been used to manage at least 76 unique campaigns that this operation has discovered. Operation SMN partners believe that many more organizations have been affected by Axiom, but are currently unaware of any compromise due to Axiom’s hyper targeting and stealth at this stage of activities,” the report says.

#Operation SMN, #Axiom, #cyber espionage, #Hikit

HOT RIGHT NOW

Samsung May Never Launch Another Note: The company will just focus on foldables and the Galaxy S

Google Paid $8.7 Million in Bug Bounties Last Year: Company says its vulnerability rewards program is growing

The Windows 11 Taskbar Is Finally Getting More Features: Microsoft working on bringing drag and drop support back

Apple Releases iOS 15.3.1, And You Need to Install It ASAP: The update includes an important security fix

Here’s How Much Samsung’s Galaxy S22 Models Will Cost in the U.S.: Full U.S. pricing information for the Galaxy S22

Samsung Launches the Galaxy S22: The all-new Galaxy S22 is finally official

Diplomacy Is Not an Option Preview (PC): The peasants are angry, and they attack in waves

Click to load comments

This enables Disqus, Inc. to process some of your data. Disqus privacy policy

Which is the best Chinese Smartphone?

Related Stories

Axiom APT group serves China's strategic interests

Sophisticated Chinese Espionage Group After Western Advanced Technology

Very specific victims targeted through spear phishing

Sednit Malware Used in Operation Pawn Storm Espionage Campaign

Vulnerability affects all Windows versions save Server 2003

New Windows Zero-Day Flaw Leveraged in the Wild

Installing the patched version is an urgent matter

Highly Critical SQL Injection Flaw in Drupal Is Easy to Exploit, Leveraged in the Wild

Individuals connected to cyber espionage also present

FBI Calls for Help Catching Cyber Offenders

Fresh Reviews

The wait was long, but DW9E is finally here

Dynasty Warriors 9: Empires Review (PS5)

The poor man’s Final Fantasy, no more, no less

Edge of Eternity Review (PS5)

Black and white FPS with old-school mechanics

Kingdom of the Dead Review (PC)

Kung fu at its best with memorable gameplay and art style

Sifu Review (PS5)

A modern take on classic RPG with a Celtic twist

The Waylanders Review (PC)

Latest News

Apple Support app updated with welcome functionality

Apple Support App Now Letting Users How Much They Have to Pay for Repairs

The ad, however, landed after the Superbowl

Microsoft Releases Surface Ad to Highlight NFL Partnership

But it’s pretty much the only thing you’re getting

Windows 11 Running on a Pixel 6 Isn’t Exactly the Windows Phone You Want

The feature is powered by a partnership with Yat

Opera Becomes the First Browser to Allow Emoji-Only Addresses

The company says it’s working on dealing with stock issues

Samsung Pauses Galaxy Tab S8 Pre-Orders Due to Massive Demand

The company says everything is returning to normal

Microsoft Will Fully Open Its Washington Offices This Month

The wait was long, but DW9E is finally here

Dynasty Warriors 9: Empires Review (PS5)

Company founder reiterates the short-term commitment

Xiaomi Wants to Become the Number One Apple Rival

The company will just focus on foldables and the Galaxy S

Samsung May Never Launch Another Note