FBI Quietly Admits to Multi-Year APT Attack, Sensitive Data Stolen

By Tom Spring

Published: 2016-04-07 · Archived: 2026-04-05 13:45:58 UTC

FBI owns up to state-sponsored hackers, known as APT6, who have infiltrated government systems for years pilfering sensitive data.

The FBI issued a rare bulletin admitting that a group named Advanced Persistent Threat 6 (APT6) hacked into US government computer systems as far back as 2011 and for years stole sensitive data.

The FBI alert was issued in February and went largely unnoticed. Nearly a month later, security experts are now shining a bright light on the alert and the mysterious group behind the attack.

“This is a rare alert and a little late, but one that is welcomed by all security vendors as it offers a chance to mitigate their customers and also collaborate further in what appears to be an ongoing FBI investigation,” said Deepen Desai, director of security research at the security firm Zscaler in an email to Threatpost.

Details regarding the actual attack and what government systems were infected are scant. Government officials said they knew the initial attack occurred in 2011, but are unaware of who specifically is behind the attacks.

“Given the nature of malware payload involved and the duration of this compromise being unnoticed – the scope of lateral movement inside the compromised network is very high possibly exposing all the critical systems,” Deepen said.

In its February bulletin, the FBI wrote: “The FBI has obtained and validated information regarding a group of malicious cyber actors who have compromised and stolen sensitive information from various government and commercial networks.

The FBI said the “group of malicious cyber actors” (known as APT6 or 1.php) used dedicated top-level domains in conjunction with the command and control servers to deliver “customized malicious software” to government computer systems. A list of domains is listed in the bulletin.

“These domains have also been used to host malicious files – often through embedded links in spear phish emails. Any activity related to these domains detected on a network should be considered an indication of a compromise requiring mitigation and contact with law enforcement,” wrote the FBI in its bulletin.

When asked for attack specifics, the FBI declined Threatpost’s request for an interview. Instead, FBI representatives issued a statement calling the alert a routine advisory aimed at notifying system administrators of persistent cyber criminals. “The release was important to add credibility and urgency to the private sector announcements and ensure that the message reached all members of the cyber-security information sharing networks,” wrote the FBI.

Deepen told Threatpost the group has been operating since at least since 2008 and has targeted China and US relations experts, Defense Department entities, and geospatial groups within the federal government. According to Deepen, APT6 has been using spear phishing in tandem with malicious PDF and ZIP attachments or links to malware infected websites that contains a malicious SCR file. The payload, Deepen said, is often the Poison Ivy remote access tool/Trojan or similar. He said the group has varied its command-and-control check-in behavior, but it is typically web-based and sometimes over HTTPS.

Experts believe that attacks are widespread and not limited to the US federal government systems. “The same or similar actors are compromising numerous organizations in order to steal sensitive intellectual property,” wrote Zscaler in a past report on APT6.

In December 2014, US government systems were compromised by hackers who broke into the Office of Personnel Management computer systems. That data breach, where 18 million people had their personal identifiable information stolen, didn’t come to light until months later in June of 2015.
