Operation Lotus Blossom: A New Nation-State Cyberthreat?

unit42.paloaltonetworks.com/operation-lotus-blossom/

Unit 42 June 16, 2015

By Unit 42

June 16, 2015 at 5:00 AM

Category: Announcement, Malware, Security Platform, Threat Prevention, Unit 42

Tags: AutoFocus, Elise, Lotus Blossom, WildFire

Today Unit 42 published new research identifying a persistent cyber espionage campaign targeting government and military organizations in Southeast Asia. The adversary group responsible for the campaign, which we named “Lotus Blossom,” is well organized and likely state-sponsored, with support from a country that has interests in Southeast Asia. The campaign has been in operation for some time; we have identified over 50 different attacks taking place over the past three years.

Background and Findings

Unit 42 has linked more than 50 individual attacks across Hong Kong, Taiwan, Vietnam, the Philippines, and Indonesia to the Lotus Blossom group. These attacks share a number of characteristics, including:

- They are against military and government targets
- Spearphishing is used as the initial attack vector
- They use a custom Trojan backdoor named “Elise” to gain a foothold
- A decoy file appears during initial compromise with Elise, tricking users into thinking they opened a benign file

Attacks by the Lotus Blossom group rely heavily on the use of spearphishing emails that use enticing subject lines and legitimate-looking decoy documents to trick users into opening a malware executable they think is a legitimate document. This document is usually a personnel roster for a specific military or government office.

We believe that the Lotus Blossom group developed the Elise malware specifically to meet the needs of the attack campaigns, and we’ve observed three variants across 50 samples during the three-year period of these attacks. Elise is a relatively sophisticated tool, including variants with the ability to evade detection in virtual environments, connect to command-and-control servers for additional instruction, and exfiltrate data.

Operation Lotus Blossom is a prime example of how a well-resourced adversary will deploy advanced tools, over an extended time period, sometimes years, in order to reach its goals. In this case, the pattern of behavior suggests that the actors behind this group were nation-state sponsored, from a country with an interest in the government and military affairs of Southeast Asian nations.

Unit 42 discovered this attack using the Palo Alto Networks AutoFocus service, which allows analysts to quickly find correlations among malware samples analyzed by WildFire. Palo Alto Networks customers are protected from the malware used in Operation Lotus Blossom via WildFire and our Security Platform’s Threat Prevention capabilities (IPS signature 14358).

We recommend that other security practitioners review the Indicators of Compromise (IoCs) in the full report to ensure they have not been targets in this campaign, and add the appropriate security controls to prevent future attacks.

The full report on Lotus Blossom from Unit 42 can be downloaded here, which includes all IOCs. The IOCs are also accessible via GitHub.

Visit Unit 42 for new research and a full list of speaking appearances, as well to subscribe to updates.