EXECUTIVE SUMMARY

OPERATION LOTUS BLOSSOM

unit 42

REPORT BY – ROBERT FALCONE, JOSH GRUNZWEIG, JEN MILLER-OSBORN, RYAN OLSON

Unit 42, the Palo Alto Networks® threat intelligence team, identified a persistent cyber espionage campaign targeting government and military organizations in Southeast Asia, with operations stretching back three years to 2012. The adversary group, which we have named "Lotus Blossom," is likely state-sponsored, with support from a country that has interests in Southeast Asia.

WELL-ORGANIZED ATTACK

During the course of Unit 42's analysis, the Lotus Blossom group was observed to deploy sophisticated attack tools, exhibiting extensive resources and persistence spanning multiple years, which suggests a well-organized team, consistent with cyber espionage conducted by nation states. Furthermore, the government and military nature of the targets, and the intelligence that could be stolen, fits with the goals of state-sponsored attacks that have been observed in the past.

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, such as:

- Military and government targets.
- Spear phishing as the initial attack vector.
- Use of a custom Trojan backdoor named "Elise" to establish an initial foothold.
- Displaying a decoy file during initial compromise with Elise, tricking users into thinking they opened a benign file.

The Lotus Blossom operation relies heavily on spear phishing as the initial attack vector, with enticing subject lines and legitimate-looking decoy documents meant to trick users into believing they are opening a legitimate file, as opposed to malware. A popular theme for the decoy documents was personnel rosters, largely claiming to be for specific military or government offices.

paloalto NETWORKS®

POSSIBLE NATION-STATE SPONSORED ATTACKS

We believe that the Lotus Blossom group developed the Elise malware specifically to meet the needs of the attack campaigns, and Unit 42 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 their 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. This type of attack, and nation-state sponsorship, isn't just applicable to Southeast Asia though, and organizations around the globe should be aware of the potential impact of an advanced adversary as such on their networks.

SHARING THREAT INTELLIGENCE IS THE BEST PREVENTION

Palo Alto Networks believes the best way to prevent incidents like this in the future is by sharing threat intelligence, thereby providing an ever-increasing positive network effect, as more and more security data is seen and consumed by a global community industry-wide. Once the adversaries' tactics, techniques and procedures are shared and widely known, they will be forced to re-tool their efforts at significant expense. By raising the cost for the attackers, we can potentially force them to look elsewhere for an easier victim, or make it too expensive for them to conduct operations at all. To this end, Unit 42 is exposing operation Lotus Blossom, and providing all related indicators, in the hope that security organizations around the globe will verify they have not been impacted and add appropriate security controls to prevent future attacks.

Unit 42 discovered this attack using the Palo Alto Networks AutoFocus™ service, which quickly allows analysts to find connections between malware samples analyzed by our WildFire™ service. When combined with open source intelligence, the team was able to increase the scope of their analysis and profile the adversary, their actions, and possible intentions. Palo Alto Networks customers are protected from the malware used in operation Lotus Blossom via WildFire and Threat Prevention (IPS signature 14358).

The full report contains detailed analysis of the specific attacks across Hong Kong, Taiwan, Vietnam, the Philippines, and Indonesia, as well as the three Elise malware variants and all related indicators of compromise (IOCs).

Read more details of the Lotus Blossom attacks on the Unit 42 BLOG.

Access the COMPLETE REPORT here, including all Indicators of Compromise (IOCs).

Subscribe to Unit 42 research and analysis UPDATES.

Learn more about AUTOFOCUS.

Learn more about WILDFIRE.

unit42

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com