Russian Attackers Exploited Windows Flaws in Attacks on European Firms

Analysis of the infrastructure used by the attackers led to the discovery of an executable named comahawk.exe that incorporated two local privilege escalation exploits targeting Windows.

The vulnerabilities, tracked as CVE-2019-1405 and CVE-2019-1322, were patched by Microsoft in November 2019 and October 2019, respectively. Microsoft's advisories for both these flaws say exploitation is less likely.

In mid-November 2019, NCC Group, whose researchers reported the vulnerabilities to Microsoft, published a blog post describing the weaknesses. Shortly after, someone made public an exploit named COMahawk that weaponizes CVE-2019-1405 and CVE-2019-1322.

Global insurer Chubb hit by Maze ransomware: claim

According to its own website, Chubb had more than US$177 billion (A$291 billion) in assets and reported US$40 billion of gross premiums in 2019. The company says it has offices in Zurich, New York, London, Paris and other locations, and has more than 30,000 employees.

iTWire contacted Chubb's Australian office for comment. A spokesperson responded: "We are currently investigating a computer security incident that may involve unauthorised access to data held by a third-party service provider.

Operation Poisoned News: Hong Kong Users Targeted With Mobile Malware via Local News Links
A recently discovered watering hole attack has been targeting iOS users in Hong Kong. The campaign uses links posted on multiple forums that supposedly lead to various news stories. While these links lead users to the actual news sites, they also use a hidden iframe to load and execute malicious code. The malicious code contains exploits that target vulnerabilities present in iOS 12.1 and 12.2. Users that click on these links with at-risk devices will download a new iOS malware variant, which we have called lightSpy (detected as IOS_LightSpy.A).

Source URL: [http://www.tuxmachines.org/node/135747](http://www.tuxmachines.org/node/135747)

Links:
[1] [http://www.tuxmachines.org/taxonomy/term/59](http://www.tuxmachines.org/taxonomy/term/59)