The Dukes: 7 Years Of Russian Cyber-Espionage

labsblog.f-secure.com/2015/09/17/the-dukes-7-years-of-russian-cyber-espionage/

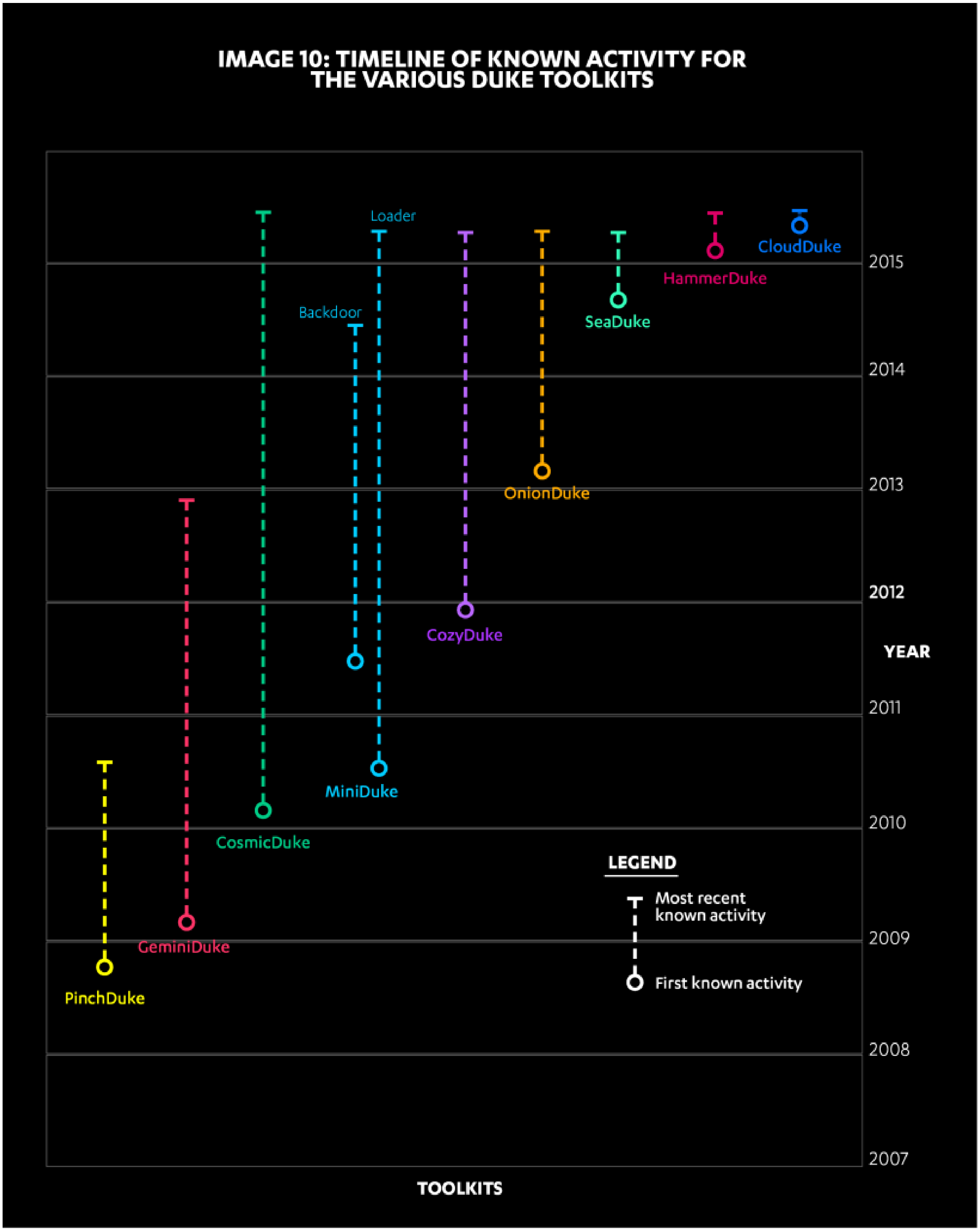
September 17, 2015

Today we release a new whitepaper on an APT group commonly referred to as "the Dukes". We believe that the Dukes are a well-resourced, highly dedicated, and organized cyber-espionage group that has been working for the Russian government since at least 2008 to collect intelligence in support of foreign and security policy decision-making.

The Dukes (sometimes also referred to as APT29) are known to employ a wide arsenal of malware toolsets including MiniDuke, CosmicDuke, OnionDuke, CozyDuke, SeaDuke, CloudDuke (aka MiniDionis), and HammerDuke (aka HAMMERTOSS [PDF]).

Despite the extensive technical research by us and others into many of the toolsets of the Dukes, we felt that we were still missing crucial parts of the story. Meanwhile, others had envisioned how the story might look, but had concluded that "it is difficult to lead the defense against that which one is not aware of or does not comprehend." (Maldre, 2015)

With this in mind, we recently set out on a journey back through all of our previous research on the Dukes looking for clues and threads that we might have missed or whose importance we might not have understood at the time. Through this process, we were able to uncover clues pointing to the existence of two previously unidentified Duke malware toolsets, PinchDuke and GeminiDuke.



While we had previously analyzed malware from both toolsets, what we hadn't understood at the time was their context. With the discovery of new clues such as these two toolsets, we went rummaging through our troves of old malware searching for cases that we had previously not known to attribute to the Dukes. Through this process of proverbial connect-the-dots, we were able to slowly build a bigger, better picture of the Dukes and uncover new details of their over 7 years of activities.

The whitepaper [PDF], with all of these juicy details (plus sample hashes), is available here.

THE DUKES

7 years of Russian cyberespionage

TLP: WHITE

This whitepaper explores the tools - such as MiniDuke, CosmicDuke, OnionDuke, CozyDuke, etc- of **the Dukes**, a well-resourced, highly dedicated and organized cyberespionage group that we believe has been working for the Russian Federation since at least 2008 to collect intelligence in support of foreign and security policy decision-making.

F-SECURE LABS
THREAT INTELLIGENCE
Whitepaper

F-Secure.

Categories

Threats & Research