Tools Used by Lamberts APT Found in Vault 7 Dumps

By Michael Mimoso

Published: 2017-04-11 · Archived: 2026-04-05 22:50:50 UTC

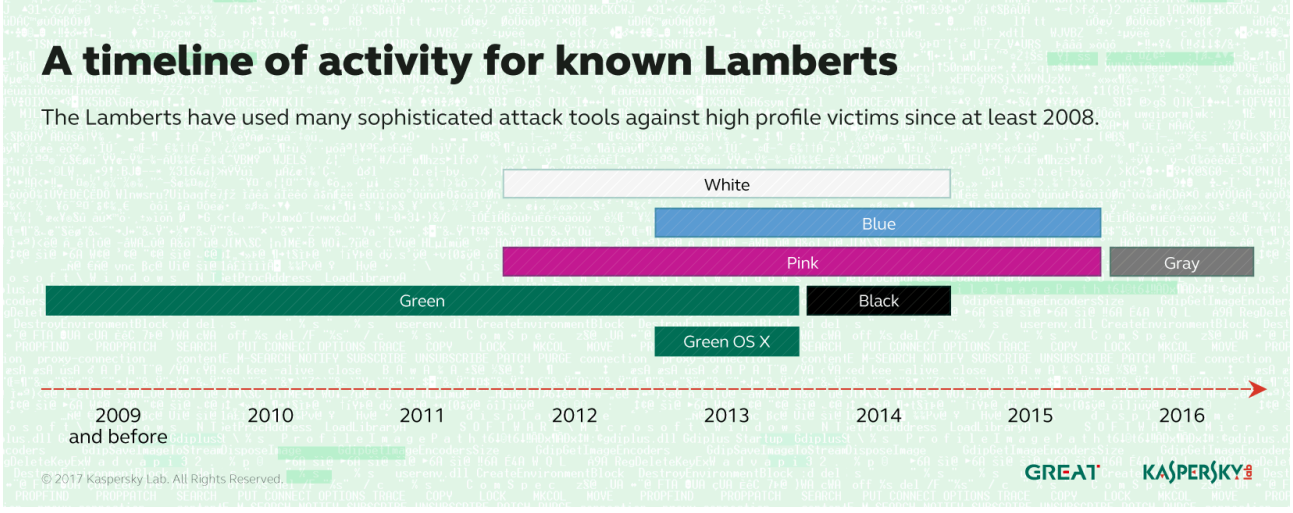
Researchers at Kaspersky Lab today disclosed the activities of the Lamberts APT, a group using many of the tools and tactics found in the Vault 7 dumps.

Links have emerged connecting targeted attacks going back a decade against high-profile government, industrial and financial targets around the world to hacking tools and documents leaked in the Vault 7 dump.

Researchers at Kaspersky Lab today published a technical report on the activities of a group it calls the Lamberts, which they say is the same group Symantec identifies as Longhorn. The Lamberts' toolkit is on par with malware and backdoors used by other APT operations such as Regin, Project Sauron, Duqu2 and Project Sauron, Kaspersky researchers said. And they added the group was most active in 2013 and 2014, but samples created last year have been discovered.

The toolkit includes memory-resident malware plugins, exploits against signed Windows drivers, network-driven backdoors, modular backdoors, data-harvesting tools and destructive wiper malware. Kaspersky researchers said that Windows and Mac OS X versions of numerous tools have been discovered as recently as last year, and that there are likely versions for other platforms Linux.

The Lamberts toolkit features six color-coded versions, according to Kaspersky. For example, Black Lambert, a malware implant, was found in a 2014 targeted attack against European organizations. This is one of the few known infection vectors used by this APT group, researchers said. In this case, the attackers exploited a zero-day vulnerability in Windows True Type Font by spreading a malicious TTF in an Office document attachment. The malicious font file was processed in kernel mode, giving the attacker remote access deep inside the compromised machine.



In analyzing Black Lambert, researchers found details such as a build number and version name that led them to White Lambert, a passive network-drive backdoor that contained similar internal configurations. White Lambert runs in kernel mode and sniffs network traffic, and receives instructions from a command and control server.

“White Lambert samples run in kernel mode and sniff network traffic looking for special packets containing instructions to execute. To run unsigned code in kernel mode on 64-bit Windows, White Lambert uses an exploit against a signed, legitimate SiSoftware Sandra driver,” the researchers wrote. “The same method was used before by Turla, ProjectSauron, and Equation’s Grayfish, with other known, legitimate drivers.”

Analysis of Black Lambert also exposed Blue Lambert, a second stage malware attack against a Black Lambert victim. Blue Lambert also exposed a number of operation or victim codenames that reference popular culture, including DOUBLESIDED SCOOBYSNACK, FUNNELCAKE CARNIVAL, RINGTOSS CARNIVAL and others.

The researchers also found Green Lambert, an older version of the Blue Lambert malware. Signatures developed for Green Lambert also triggered an OS X version of the malware.

“The OS X variant of Green Lambert is in many regards functionally identical to the Windows version, however it misses certain functionality such as running plugins directly in memory,” the Kaspersky researchers wrote.

Pink Lambert is another set of attack tools that includes a beaconing implant, USB-harvesting capabilities and a framework used to write malware that runs regardless of platform. Kaspersky Lab said it found Pink Lambert on systems infected with White Lambert.

The newest version of the Lamberts’ malware, Gray Lambert, has a similar coding style to Pink Lambert and includes updated versions of much of the same types of capabilities.

The Lamberts, or Longhorn, employ a number of the same crypto protocols and means of evading detection by security software as described in the Vault 7 dumps allegedly tied to the CIA by Wikileaks.

The dumps of thousands of documents started March 7, and included malware, weaponized zero-day exploits, remote access Trojans and related documentations. Wikileaks claims this is the CIA’s entire hacking catalogue. Cisco and other vendors have begun patching some of the zero days released in the Year Zero dump.

A second release on March 23, called Dark Matter, included a capabilities focusing on Apple platforms, including tracking iPhone users and developing implants and exploits for Mac OS X firmware.

“The fact that in the vast majority of cases the infection method is unknown probably means there are still a lot of unknown details about these attacks and the group(s) leveraging them,” the researchers wrote.

Source: https://threatpost.com/tools-used-by-lamberts-apt-found-in-vault-7-dumps/124900/