

Unraveling the Lamberts Toolkit

SL securelist.com/blog/research/77990/unraveling-the-lamberts-toolkit/



Authors



An Overview of a Color-coded Multi-Stage Arsenal

Yesterday, our colleagues from [Symantec](#) published their [analysis of Longhorn](#), an advanced threat actor that can be easily compared with Regin, ProjectSauron, Equation or Duqu2 in terms of its complexity.

Longhorn, which we internally refer to as “The Lamberts”, first came to the attention of the ITSec community in 2014, when our colleagues from [FireEye](#) [discovered an attack using a zero day vulnerability \(CVE-2014-4148\)](#). The attack leveraged malware we called ‘BlackLambert’, which was used to target a high profile organization in Europe.

Since at least 2008, The Lamberts have used multiple sophisticated attack tools against high-profile victims. Their arsenal includes network-driven backdoors, several generations of modular backdoors, harvesting tools, and wipers. Versions for both Windows and OSX are known at this time, with the latest samples created in 2016.

Although the operational security displayed by actors using the Lamberts toolkit is very good, one sample includes a PDB path that points to a project named “Archan~1” (perhaps ‘Archangel’). The root folder on the PDB path is named “Hudson”. This is one of the very few mistakes we’ve seen with this threat actor.

While in most cases the infection vector remains unknown, the high profile attack from 2014 used a very complex Windows TTF zero-day exploit (CVE-2014-4148).

Kaspersky Lab products successfully detect and eradicate all the known malware from the Lamberts family. For more information please contact: intelreports@kaspersky.com

An Overview of the Lamberts



Figure 1. Lamberts discovery timeline

The first time the Lambert family malware was uncovered publicly was in October 2014, when FireEye [posted](#) a blog about a zero day exploit (CVE-2014-4148) used in the wild. The vulnerability was patched by Microsoft at the same time. We named the malware involved ‘Black Lambert’ and described it thoroughly in a private report, available to Kaspersky APT Intel Reports subscribers.

The authors of Black Lambert included a couple of very interesting details in the sample, which read as the following: **toolType=wl**, **build=132914**, **versionName = 2.0.0**. Looking for similar samples, we were able to identify another generation of related tools which we called White Lambert. While Black Lambert connects directly to its C&C for instructions, White Lambert is a fully passive, network-driven backdoor.

	Black Lambert	White Lambert
Implant type	Active	Passive
toolType	wl	aa (“ArchAngel”)
build	132914	113140
versionName	2.0.0	5.0.2

Internal configuration similarities in Black and White Lambert

White Lambert runs in kernel mode and intercepts network traffic on infected machines. It decrypts packets crafted in a special format to extract instructions. We named these passive backdoors ‘White Lambert’ to contrast with the active “Black Lambert” implants.

Looking further for any other malware related to White Lambert and Black Lambert, we came by another generation of malware that we called Blue Lambert.

One of the Blue Lambert samples is interesting because it appears to have been used as second stage malware in a high profile attack, which involved the Black Lambert malware.

Looking further for malware similar to Blue Lambert, we came by another family of malware we called Green Lambert. Green Lambert is a lighter, more reliable, but older version of Blue Lambert. Interestingly, while most Blue Lambert variants have version numbers in the range of 2.x, Green Lambert is mostly in 3.x versions. This stands in opposition to the data gathered from export timestamps and C&C domain activity that points to Green Lambert being considerably older than the Blue variant. Perhaps both Blue and Green Lamberts have been developed in parallel by two different teams working under the same umbrella, as normal software version iterations, with one seeing earlier deployment than the other.

Signatures created for Green Lambert (Windows) have also triggered on an OS X variant of Green Lambert, with a very low version number: 1.2.0. This was uploaded to a multiscanner service in September 2014. 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.

Kaspersky Lab detections for Blue, Black, and Green Lamberts have been triggered by a relatively small set of victims from around the world. While investigating one of these infections involving White Lambert (network-driven implant) and Blue Lambert (active implant), we found yet another family of tools that appear to be related. We called this new family Pink Lambert.

The Pink Lambert toolset includes a beaconing implant, a USB-harvesting module and a multi-platform orchestrator framework which can be used to create OS-independent malware. Versions of this particular orchestrator were found on other victims, together with White Lambert samples, indicating a close relationship between the White and Pink Lambert malware families.

By looking further for other undetected malware on victims of White Lambert, we found yet another apparently related family. The new family, which we called Gray Lambert is the latest iteration of the passive network tools from the Lamberts' arsenal. The coding style of Gray Lambert is similar to the Pink Lambert USB-harvesting module, however, the functionality mirrors that of White Lambert. Compared to White Lambert, Gray Lambert runs in user mode, without the need for exploiting a vulnerable signed driver to load arbitrary code on 64-bit Windows variants.

Connecting all these different families by shared code, data formats, C&C servers, and victims, we have arrived at the following overarching picture:

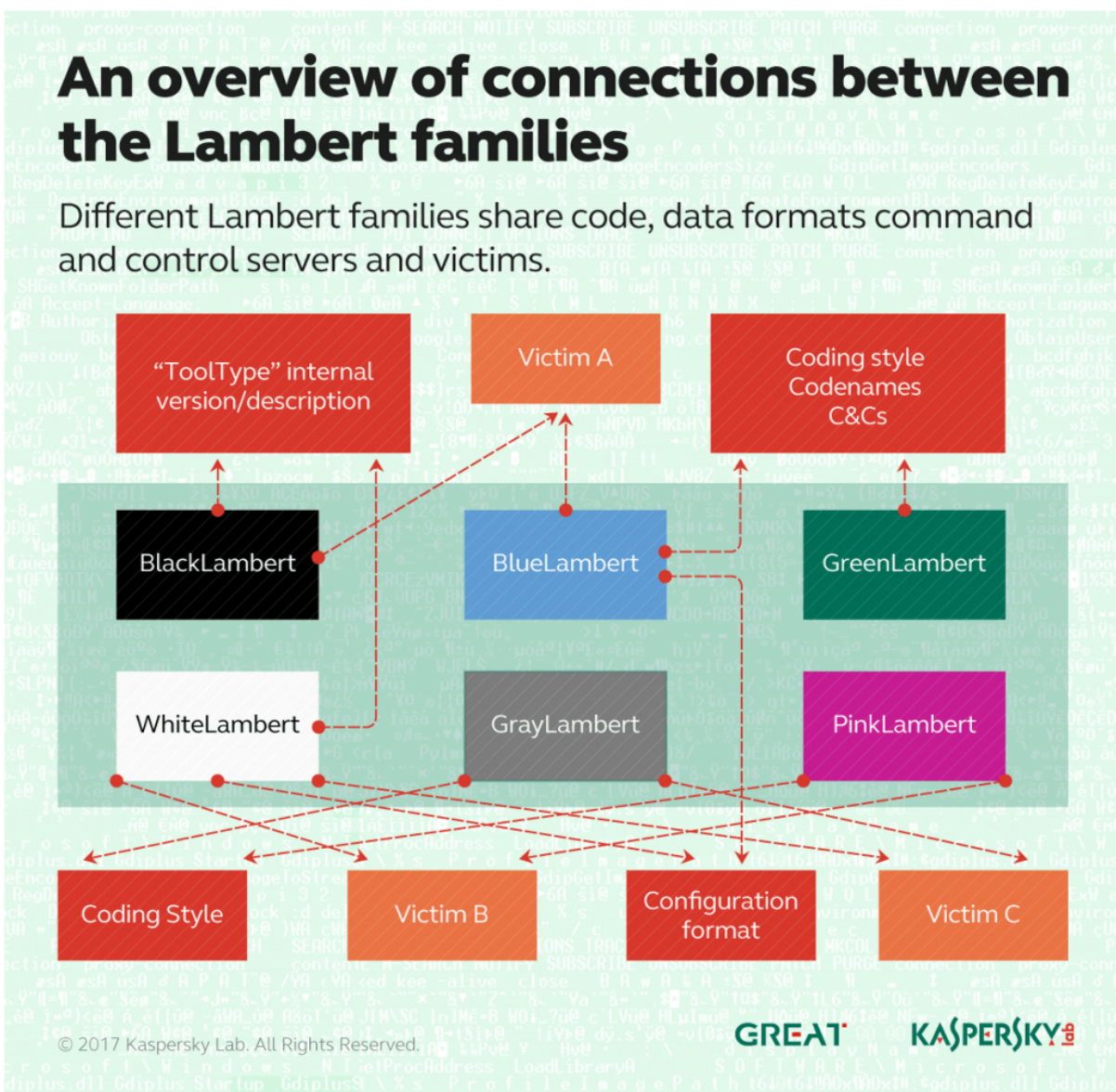


Figure 2. An overview of connections between the Lambert families

The Lamberts in Brief – from Black to Gray

Below, we provide a small summary of all the Lamberts. A full description of all variants is available to subscribers of Kaspersky APT Reports. Contact intelreports@kaspersky.com

Black Lambert

The only known sample of Black Lambert was dropped by a TTF-exploit zero day (CVE-2014-4148). Its internal configuration included a proxy server which suggests the malware was created to work in a very specific network configuration, inside the victim's network.

An internal description of Black Lambert indicates what appears to be a set of markers used by the attackers to denote this particular branch: **toolType=wl, build=132914, versionName = 2.0.0.**

Hash	Description
683afdef710bf3c96d42e6d9e7275130	generic loader (hdmsvc.exe)
79e263f78e69110c09642bbb30f09ace	winlib.dll, final payload (toolType=wl)

Blue Lambert

The Blue Lambert implants contain what appear to be version numbers in the 2.x range, together with project/operation codename sets, which may also indicate codenames for the victims or campaigns.

```
300
17
180
0
300
FUNNELCAKE
CARNIVAL
https://www2.uaefinance.org,https://103.242.119.71
[[", "]]
{"R": [[23400, 61200]], "M": [[23400, 61200]], "T": [[23400, 61200]], "W": [[23400, 61200]], "F": [[23400, 61200]]}
7
512
5
0
```

Figure 4. Blue Lambert configuration in decrypted form, highlighting internal codenames

Known codenames include TRUE CRIME (2.2.0.2), CERVELO YARDBIRD (2.6.1.1), GAI SHU (2.2.0.5), DOUBLESIDED SCOOBYSNACK (2.3.0.2), FUNNELCAKE CARNIVAL (2.5.0.2), PROSPER SPOCK (2.0.0.2), RINGTOSS CARNIVAL (2.4.2.2), COD FISH (2.2.0.0), and INVERTED SHOT (2.6.2.3).

Green Lambert

Green Lambert is a family of tools deeply related to Blue Lambert. The functionality is very similar, both Blue and Green are active implants. The configuration data shares the same style of codenames for victims, operations, or projects.

```

.0041ED80: 00 00 00 02-00 00 00 73-7A 38 00 47-72 61 70 68  ics sz8 Graph
.0041ED90: 69 63 73 20-55 74 69 6C-69 74 79 20-4D 67 6D 74  ics Utility Mgmt
.0041EDA0: 20 53 65 72-76 69 63 65-00 2E 00 00-00 02 00 00  ics Service .
.0041EDB0: 00 32 6F 69-00 4D 61 6E-61 67 65 73-20 69 6E 74  ics 2oi Manages int
.0041EDC0: 65 72 6E 61-6C 20 67 72-61 70 68 69-63 73 20 64  ernal graphics d
.0041EDD0: 72 69 76 65-72 73 00 12-00 00 00 02-00 00 00 66  ivers ↓
.0041EDE0: 69 64 00 50-49 5A 5A 41-00 14 00 00-00 02 00 00  id PIZZA
.0041EDF0: 00 6F 75 31-00 41 53 53-41 55 4C 54-00 25 00 00  ou1 ASSAULT %
.0041EE00: 00 02 00 00-00 79 30 32-00 68 74 74-70 3A 2F 2F  ics y02 http://
.0041EE10: 77 77 77 2E-6D 69 63 72-6F 73 6F 66-74 2E 63 6F  www.microsoft.co
.0041EE20: 6D 00 3C 00-00 00 02 00-00 00 69 34-67 00 68 74  m <
.0041EE30: 74 70 73 3A-2F 2F 63 64-6E 2E 66 6D-6C 73 74 61  tps://cdn.fmlsta
.0041EE40: 74 69 63 2E-63 6F 6D 7C-68 74 74 70-73 3A 2F 2F  tic.com|https://
.0041EE50: 31 32 30 2E-35 30 2E 33-38 2E 31 38-37 00 16 00  120.50.38.187
.0041EE60: 00 00 02 00-00 00 70 73-75 00 6C 6F-67 69 6E 2E  ics psu login.
.0041EE70: 70 68 70 00-18 00 00 00-02 00 00 00-34 62 6B 00  php ↑
.0041EE80: 67 65 74 63-6F 6E 66 2E-70 68 70 00-18 00 00 00  getconf.php ↑

```

Figure 5. Green Lambert configuration block (decrypted) highlighting internal codenames

The Green Lambert family is the only one where non-Windows variants have been found. An old version of Green Lambert, compiled for OS X was uploaded from Russia to a multiscanner service in 2014. Its internal codename is HO BO (1.2.0).

The Windows versions of Green Lambert have the following code names: BEARD BLUE (2.7.1), GORDON FLASH (3.0), APE ESCAPE (3.0.2), SPOCK LOGICAL (3.0.2), PIZZA ASSAULT (3.0.5), and SNOW BLOWER (3.0.5).

Interestingly, one of the droppers of Green Lambert abused an ICS software package named “Subway Environmental Simulation Program” or “SES”, which has been available on certain forums visited by engineers working with industrial software. Similar techniques have been observed in the past from other threat groups, for instance, trojanized Oracle installers by the Equation group.

White Lambert

White Lambert is a family of tools that share the same internal description as Black Lambert. Known tool types, builds, and version names include:

- ToolType “aa”, protocol 3, version 7, versionName 5.0.2, build 113140
- ToolType “aa”, protocol 3, version 7, versionName 5.0.0, build 113140
- ToolType “aa”, protocol 3, version 6, versionName 4.2.0, build 110836M
- ToolType “aa”, protocol 3, version 5, versionName 3.2.0

One of the White Lambert samples is interesting because it has a forgotten PDB path inside, which points to “Archan~1l” and “Hudson”. Hudson could point to a project name, if the authors name their projects by rivers in the US, or, it could also be the developer’s first

name. The truncated (8.3) path “archan~1” most likely means “Archangel”. The tool type “aa” could also suggest “ArchAngel”. By comparison, the Black Lambert tool type “wl” has no known meaning.

```
033E10: 28 19 C7 04 B0 5D 00 00 | 52 53 44 53 7C 0C F7 FE | (↓↵] RSDS | ♀
033E20: 48 C4 B2 4E A3 5D CB D4 | AC CE 8B AB 01 00 00 00 | HIJ>N] >>>
033E30: 63 3A 5C 68 75 64 73 6F | 6E 5C 77 6F 72 6B 73 70 | c:\hudson\worksp
033E40: 7E 32 5C 61 72 63 68 61 | 6E 7E 31 5C 74 61 72 67 | ~2\archan~1\targ
033E50: 65 74 5C 6F 62 6A 66 72 | 65 5F 77 6C 68 5F 61 6D | et\objfre_wlh_am
033E60: 64 36 34 5C 61 6D 64 36 | 34 5C 74 61 72 67 65 74 | d64\amd64\target
033E70: 2E 70 64 62 00 00 00 00 | 01 00 00 00 01 1A 02 00 | .pdb @ @→
033E80: 1A 01 1B 00 00 00 00 00 | 01 00 00 00 01 18 08 00 | →← @ @↑
```

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 same method was used before by Turla, ProjectSauron, and Equation’s Grayfish, with other known, legitimate drivers.

Pink Lambert

Pink Lambert is a suite of tools initially discovered on a White Lambert victim. It includes a beaconing implant, partially based on publicly available source code. The source code on top of which Pink Lambert’s beaconing implant was created is “A Fully Featured Windows HTTP Wrapper in C++”.


A Fully Featured Windows HTTP Wrapper in C++

shicheng, 22 Sep 2010 CPOL

Rate this: ★★★★★

★★★★★ 4.93 (92 votes)

A fully featured and easy-to-use Windows HTTP wrapper in C++

 [Download source - 32.67 KB](#)

Introduction

This is a fully featured Windows HTTP Wrapper in C++. It is a wrapper in the C++ class. It is fully featured and easy to use. You only need to include one single header file to use the wrapper.

Figure 6. “A Fully Featured Windows HTTP Wrapper” by shicheng

Other tools in the Pink Lambert suite include USB stealer modules and a very complex multi-platform orchestrator.

In a second incident, a Pink Lambert orchestrator was found on another White Lambert victim, substantiating the connection between the Pink and White Lamberts.

Gray Lambert

Gray Lambert is the most recent tool in the Lamberts' arsenal. It is a network-driven backdoor, similar in functionality to White Lambert. Unlike White Lambert, which runs in kernel mode, Gray Lambert is a user-mode implant. The compilation and coding style of Gray Lambert is similar to the Pink Lambert USB stealers. Gray Lambert initially appeared on the computers of victims infected by White Lambert, which could suggest the authors were upgrading White Lambert infections to Gray. This migration activity was last observed in October 2016.

Some of the known filenames for Gray Lambert are mwapi32.dll and poolstr.dll – it should be pointed though that the filenames used by the Lamberts are generally unique and have never been used twice.

Timeline

Most of the Blue and Green Lambert samples have two C&C servers hardcoded in their configuration block: a hostname and an IP address. Using our own pDNS as well as DomainTools IP history, we plotted the times when the C&C servers were active and pointing to the same IP address as the one from the configuration block.

Unfortunately, this method doesn't work for all samples, since some of them don't have a domain for C&C. Additionally, in some cases we couldn't find any pDNS information for the hostname configured in the malware.

Luckily, the attackers have made a few mistakes, which allow us to identify the activity times for most of the other samples. For instance, in case when no pDNS information was available for a subdomain on top of the main C&C domain, the domain registration dates were sufficient to point out when the activity began. Additionally, in some cases the top domain pointed to the same IP address as the one from the configuration file, allowing us to identify the activity times.

Another worthwhile analysis method focuses on the set of Blue Lambert samples that have exports. Although most compilation timestamps in the PE header appear to have been tampered (to reflect a 2003-2004 range), the authors forgot to alter the timestamps in the export section. This allowed us to identify not just the activity / compilation timestamps, but also the method used for faking the compilation timestamps in the PE header.

It seems the algorithm used to tamper with the samples was the following: subtract 0x10 from the highest byte of timestamp (which amounts to about 8 and half years) and then randomize the lowest 3 bytes. This way we conclude that for Blue Lamberts, that original

compilation time of samples was in the range of 2012-2015.

Putting together all the various families, with recovered activity times, we come to the following picture:

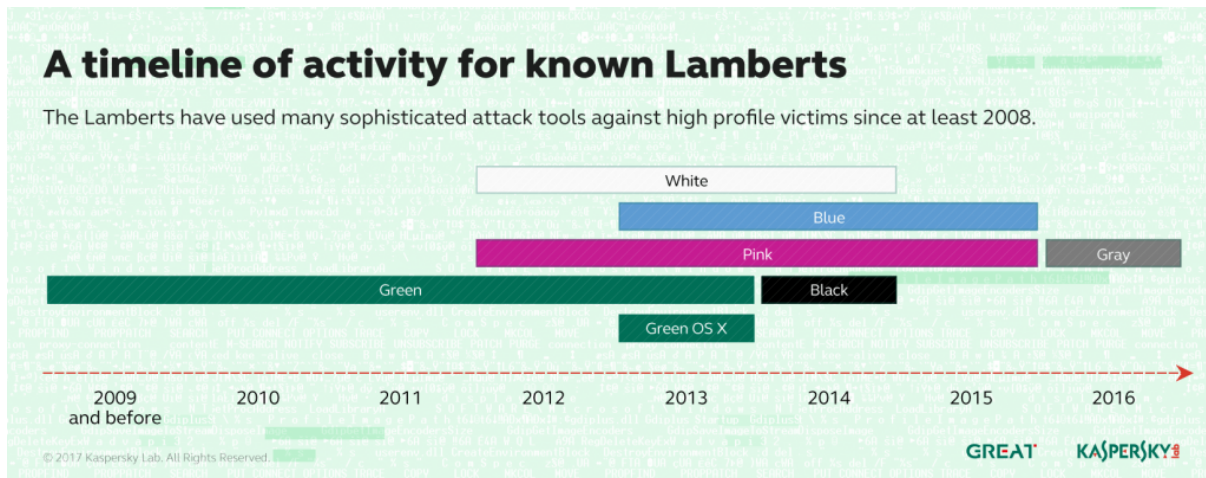


Figure 8. A timeline of activity for known Lamberts

As it can be seen from the chart above, Green Lambert is the oldest and longest-running in the family, while Gray is the newest. White, Blue and Pink somehow overlap in deployment, with Blue replacing Green Lambert. Black Lambert was seen only briefly and we assume it was “retired” from the arsenal after being discovered by FireEye in 2014.

Codenames and Popular Culture Referenced in Lamberts

The threat group(s) behind the Lambert toolkits have used a large number of codenames extensively throughout their projects. Some of these codenames are references to old computer games, Star Trek, and cartoons, which is very unusual for high profile APT groups. We really enjoyed going through the backstories of these codenames and wanted to provide them below for others to enjoy as well.

For instance, one of the Green Lambert versions has the internal codename “GORDON FLASH”, which can also be read as “FLASH GORDON”. Flash Gordon is the hero of a space opera adventure comic strip created by and originally drawn by Alex Raymond. It was first published in 1934 and subsequently turned into a popular film in 1980.



Flash Gordon poster

A 'Funnel cake' is a regional food popular in North America at carnivals, fairs, sporting events, and seaside resorts. This explains the codename "FUNNELCAKE CARNIVAL":



Figure 9. A typical funnel cake

Spock and Prosper obviously refers to Star Trek, the well-known science fiction television series created by Gene Roddenberry. Cdr. Spock is a half-Vulcan, half-human character, portrayed by Leonard Nimoy. "Live long and prosper" is the traditional Vulcan greeting in the series.



Leonard Nimoy as "Spock" displaying the traditional Vulcan greeting "Live long and prosper"

Ringtoss is a game that is very popular at carnivals in North America.



DOUBLESIDED SCOOBYSNACK is likely a reference to an NFL Lip Reading video featuring Adrian Peterson that went viral in mid-2013. According to the urban dictionary, it is also used to denote a sexual game in which the participants are dressed as Scooby-Doo and his master.

Ape Escape (also known as Saru Get You (サルゲッチュ Saru Getchu) in Japan) is a series of video games made by SCE Japan Studio, starting with Ape Escape for PlayStation in 1999. The series often incorporates ape-related humor, unique gameplay, and a wide variety of pop culture references; it is also notable for being the first game to make the DualShock or Dual Analog controller mandatory.



Ape Escape

INVERTED SHOT is likely a reference to a mixed martial arts move also known as an 'Imanari roll takedown', named after Masakazu Imanari who popularized the grappling technique. It consists of a modified Brazilian jiu-jitsu granby roll that places the fighter in inverted guard position while taking the opponent down to the mat.

GAI and SHU (as used in Green Lambert OS X) are characters from the Guilty Crown anime series. Gai Tsutsugami (恙神 涯 Tsutsugami Gai) is the 17-year-old resourceful and charismatic leader of the "Funeral Parlor" resistance group, while Shu Ouma (桜満 集 Ōma Shū) is the 17-year-old main protagonist of Guilty Crown.



Figure 10. Main characters of Guilty Crown with Shu Ouma in the middle.

Conclusions

The Lamberts toolkit spans across several years, with most activity occurring in 2013 and 2014. Overall, the toolkit includes highly sophisticated malware, which relies on high-level techniques to sniff network traffic, run plugins in memory without touching the disk, and leverages exploits against signed drivers to run unsigned code on 64-bit Windows.

To further exemplify the proficiency of the attackers leveraging the Lamberts toolkit, deployment of Black Lambert included a rather sophisticated TTF zero day exploit, CVE-2014-4148. Taking that into account, we classify the Lamberts as the same level of complexity as Regin, ProjectSauron, Equation and Duqu2, which makes them one of the most sophisticated cyber espionage toolkits we have ever analysed.

Considering the complexity of these projects and the existence of an implant for OS X, we assume that it is highly possible that other Lamberts also exist for other platforms, such as Linux. 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.

As usual, defense against attacks such as those from the Lamberts/Longhorn should include a multi-layered approach. Kaspersky products include special mitigation strategies against the malware used by this group, as well as the many other APT groups we track. If you are interested in reading more about effective mitigation strategies in general, we recommend the following articles:

- [Strategies for mitigating APTs](#)
- [How to mitigate 85% of threats with four strategies](#)

We will continue tracking the Lamberts and sharing new findings with our intel report subscribers, as well as with the general public. If you would like to be the first to hear our news, we suggest you subscribe to our intel reports.

Kaspersky Lab products successfully detect and eradicate all the known malware from the Lamberts family.

For more information about the Lamberts, please contact: intelreports@kaspersky.com

- [APT](#)
- [Backdoor](#)
- [Malware Descriptions](#)
- [Targeted attacks](#)
- [Zero-day vulnerabilities](#)

Authors



Unraveling the Lamberts Toolkit

Your email address will not be published. Required fields are marked *