January 2004 to September 2015

f-secure.com/weblog/archives/00002822.html

F-SECURE LABS

<<< NEWS FROM THE LAB - Wednesday, July 22, 2015 >>>

ARCHIVES | **SEARCH**

Duke APT group's latest tools: cloud services and Linux support Posted by Artturi @ 11:59 GMT

Recent weeks have seen the outing of two new additions to the Duke group's toolset, SeaDuke and CloudDuke. Of these, SeaDuke is a simple trojan made interesting by the fact that it's written in Python. And even more curiously, SeaDuke, with its built-in support for both Windows and Linux, is the first cross-platform malware we have observed from the Duke group. While SeaDuke is a single - albeit cross-platform - trojan, CloudDuke appears to be an entire toolset of malware components, or "solutions" as the Duke group apparently calls them. These components include a unique loader, downloader, and not one but two different trojan components. CloudDuke also greatly expands on the Duke group's usage of cloud storage services, specifically Microsoft's OneDrive, as a channel for both command and control as well as the exfiltration of stolen data. Finally, some of the recent CloudDuke spear-phishing campaigns have born a striking resemblance to CozyDuke spear-phishing campaigns from a year ago.

Linux support added with the cross-platform SeaDuke malware

Last week, both Symantec and Palo Alto Networks published research on SeaDuke, a newer addition to the arsenal of trojans being used by the Duke group. While older malware by the Duke group has always been written with a combination of the C and C++ programming languages as well as assembly language, SeaDuke is peculiarly written in Python with multiple layers of obfuscation. This Python code is usually then compiled into Windows executables using py2exe or pyinstaller. However, the Python

code itself has been designed to work on both Windows and Linux. We therefore suspect, that the Duke group is also using the same SeaDuke Python code to target Linux victims. This is the first time we have seen the Duke group employ malware to target Linux platforms.

```
@property
def autoload_settings(self):
 windows_autoload_settings={'exe_name':'iexplore.exe','app_name':'Internet Explorer','self_delete':False}
 linux_autoload_settings={'exe_name':'httpd','app_name':'Apache','self_delete':False}
 if sys_platform=='win32':
  default_autoload_settings=windows_autoload_settings
 else:
  default_autoload_settings=linux_autoload_settings
 return v_conf_json.get('autoload_settings',default_autoload_settings)
```

An example of the cross-platform support found in SeaDuke.

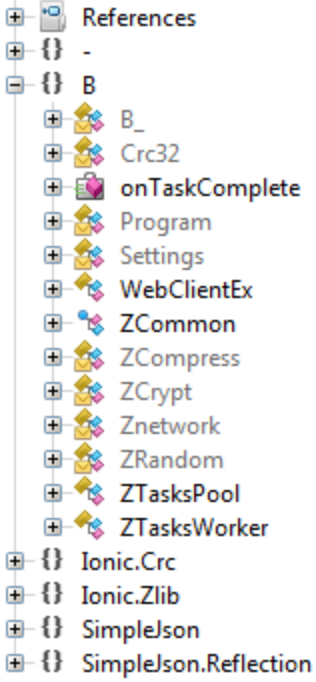
A new set of solutions with the CloudDuke malware toolset

Last week, we also saw Palo Alto Networks and Kaspersky Labs publish research on malware components they respectively called MiniDionis and CloudLook. MiniDionis and CloudLook are both components of a larger malware toolset we call CloudDuke. This toolset consists of malware components that provide varying functionality while partially relying on a shared code framework and always using the same loader. Based on PDB strings found in the samples, the malware authors refer to the CloudDuke components as "solutions" with names such as "DropperSolution", "BastionSolution" and "OneDriveSolution". A list of PDB strings we have observed is below:

C:\DropperSolution\Droppers\Projects\Drop_v2\Release\Drop_v2.pdb
c:\BastionSolution\Shells\Projects\miniDionis4\miniDionis\obj\Release\miniDionis.pdb
c:\BastionSolution\Shells\Projects\miniDionis2\miniDionis\obj\Release\miniDionis.pdb
c:\OneDriveSolution\Shells\Projects\OneDrive2\OneDrive\obj\x64\Release\OneDrive.pdb

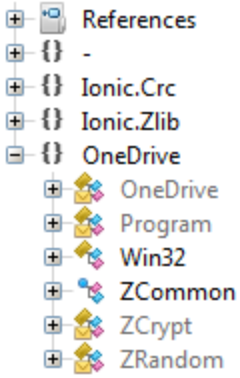
The first of the CloudDuke components we have observed is a downloader internally called "DropperSolution". The purpose of the downloader is to download and execute additional malware on the victim's system. In most observed cases, the downloader will attempt to connect to a compromised website to download an encrypted malicious payload which the downloader will decrypt and execute. Depending on the way the downloader has been configured, in some cases it may first attempt to log in to Microsoft's cloud storage service OneDrive and retrieve the payload from there. If no payload is available from OneDrive, the downloader will revert to the previously mentioned method of downloading from compromised websites.

We have also observed two distinct trojan components in the CloudDuke toolset. The first of these, internally called "BastionSolution", is the trojan that Palo Alto Networks described in their research into "MiniDionis". Interestingly, BastionSolution appears to functionally be an exact copy of SeaDuke with the only real difference being the choice of programming language. BastionSolution also makes significant use of a code framework that is apparently internally called "Z". This framework provides classes for functionality such as encryption, compression, randomization and network communications.



A list of classes in the BastionSolution trojan, including multiple classes from the "Z" framework.

Classes from the same "Z" framework, such as the encryption and randomization classes, are also used by the second trojan component of the CloudDuke toolset. This second component, internally called "OneDriveSolution", is especially interesting because it relies on Microsoft's cloud storage service OneDrive as its command and control channel. To achieve this, OneDriveSolution will attempt to log into OneDrive with a preconfigured username and password. If successful, OneDriveSolution will then proceed to copy data from the victim's computer to the OneDrive account. It will also search the OneDrive account for files containing commands for the malware to execute.



A list of classes in the OneDriveSolution trojan, including multiple classes from the "Z" framework.

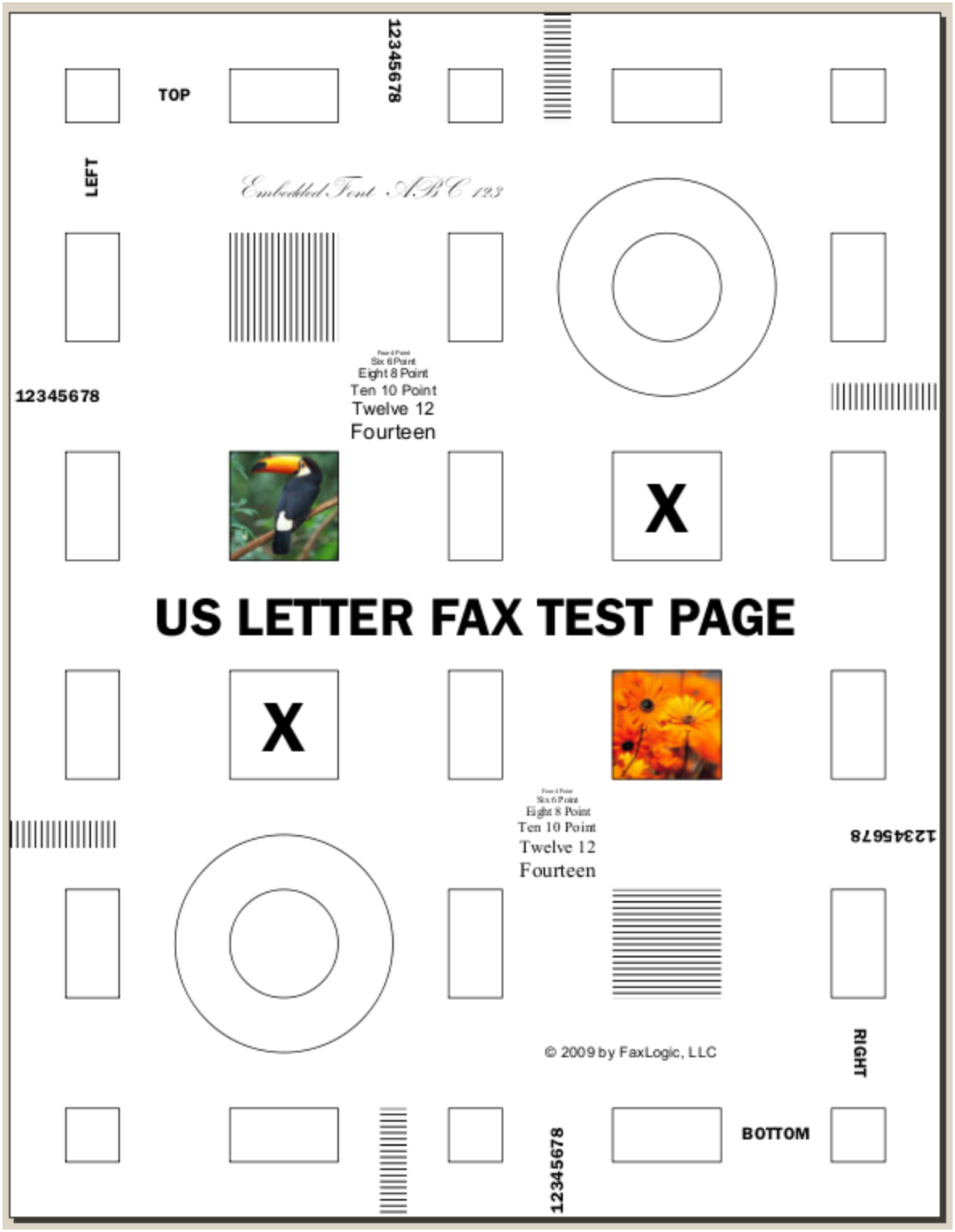
All of the CloudDuke "solutions" use the same loader, a piece of code whose primary purpose is to decrypt the embedded, encrypted solution, load it in memory and execute it. The Duke group has often employed loaders for their malware but unlike the previous loaders they have used, the CloudDuke loader is much more versatile with support for multiple methods of loading and executing the final payload as well as the ability to write to disk and execute additional malware components.

CloudDuke spear-phishing campaigns and similarities with CozyDuke

CloudDuke has recently been spread via spear-phishing emails with targets reportedly including organizations such as the US Department of Defense. These spear-phising emails have contained links to compromised websites hosting zip archives that contain CloudDuke-laden executables. In most cases, executing these executables will have resulted in two additional files being written to the victim's hard disk. The first of these files has been a decoy, such as an audio file or a PDF file while the second one has been a CloudDuke loader embedding a CloudDuke downloader, the so-called "DropperSolution". In these cases, the victim has been presented with the decoy file while in the background the downloader has proceeded to download and execute one of the CloudDuke trojans, "OneDriveSolution" or "BastionSolution".

Example of one of the decoy documents employed in the CloudDuke spear-phishing campaigns. It has apparently been copied by the attackers from here.

Interestingly, however, some of the other CloudDuke spear-phishing campaigns we have observed this July have born a striking resemblance to CozyDuke spear-phishing campaigns seen almost exactly a year ago, in the beginning of July 2014. In both spear-phishing campaigns, the decoy document has been the exact same PDF file, a "US letter fax test page" (28d29c702fdf3c16f27b33f3e32687dd82185e8b). Similarly, the URLs hosting the malicious files have, in both campaigns, purported to be related to eFaxes. It is also interesting to note, that in the case of the CozyDuke-inspired CloudDuke spear-phishing campaign, the downloading and execution of the malicious archive linked to in the emails has not resulted in the execution of the CloudDuke downloader but in the execution of the "BastionSolution" component thereby skipping one step from the process described for the other CloudDuke spear-phishing campaigns.



The "US letter fax test page" decoy employed in both CloudDuke and CozyDuke spear-phishing campaigns.

Increasingly using cloud services to evade detection

CloudDuke is not the first time we have observed the Duke group use cloud services in general and Microsoft OneDrive specifically as part of their operations. Earlier this spring we released research on CozyDuke where we mentioned observing CozyDuke sometimes either directly use a OneDrive account to exfiltrate stolen data or alternatively

CozyDuke downloading Visual Basic scripts that would copy stolen files to a OneDrive account and sometimes even retrieve files containing additional commands from the same OneDrive account.

In these previous cases the Duke group has only used OneDrive as a secondary communication channel but still relied on more traditional C&C channels for most of their actions. It is therefore interesting to note that CloudDuke actually enables the Duke group to rely solely on OneDrive for every step of their operation from downloading the actual trojan, passing commands to the trojan and finally exfiltrating stolen data.

By relying solely on 3rd party web services, such as OneDrive, as their command and control channel, we believe the Duke group is trying to better evade detection. Large amounts of data being transferred from an organization's network to an unknown web server easily raises suspicions. However, data being transferred to a popular cloud storage service is normal. What better way for an attacker to surreptitiously transfer large amounts of stolen data than the same way people are transferring that same data every day for legitimate reasons. (Coincidentally, the implications of 3rd party web services being used as command and control channels is also the subject of an upcoming talk at the VirusBulletin 2015 conference).

Directing limited resources towards evading detection and staying ahead of defenders

Developing even a single multipurpose malware toolset, never mind many, requires time and resources. Therefore it seems logical to attempt to reuse code such as supporting frameworks between different toolsets. The Duke group, however, appear to have taken this a step further with SeaDuke and the CloudDuke component BastionSolution, by rewriting the same code in multiple programming languages. This has the obvious benefits of saving time and resources by providing two malware toolsets, that while similar on the inside, appear completely different on the outside. This way, the discovery of one toolset does not immediately lead to the discovery of the second toolset.

The Duke group, long suspected of ties to the Russian state, have been running their espionage operation for an unusually long time and - especially lately - with unusual brazenness. These latest CloudDuke and SeaDuke campaigns appear to be a clear sign that the Duke's are not planning to stop any time soon.

Research and post by Artturi (@lehtior2)

F-Secure detects CloudDuke as Trojan:W32/CloudDuke.B and Trojan:W64/CloudDuke.B

Samples:

04299c0b549d4a46154e0a754dda2bc9e43dff76
2f53bfcd2016d506674d0a05852318f9e8188ee1
317bde14307d8777d613280546f47dd0ce54f95b
476099ea132bf16fa96a5f618cb44f87446e3b02
4800d67ea326e6d037198abd3d95f4ed59449313
52d44e936388b77a0afdb21b099cf83ed6cbaa6f
6a3c2ad9919ad09ef6cdffc80940286814a0aa2c
78fbdfa6ba2b1e3c8537be48d9efc0c47f417f3c
9f5b46ee0591d3f942ccaa9c950a8bff94aa7a0f
bfe26837da22f21451f0416aa9d241f98ff1c0f8

c16529dbc2987be3ac628b9b413106e5749999ed
cc15924d37e36060faa405e5fa8f6ca15a3cace2
dea6e89e36cf5a4a216e324983cc0b8f6c58eaa8
e33e6346da14931735e73f544949a57377c6b4a0
ed0cf362c0a9de96ce49c841aa55997b4777b326
f54f4e46f5f933a96650ca5123a4c41e115a9f61
f97c5e8d018207b1d546501fe2036adfbf774cfd

Compromised servers used for command and control:

hxxps://cognimuse.cs.ntua.gr/search.php
hxxps://portal.sbn.co.th/rss.php
hxxps://97.75.120.45/news/archive.php
hxxps://portal.sbn.co.th/rss.php
hxxps://58.80.109.59/plugins/search.php

Compromised websites used to host CloudDuke:

hxxp://flockfilmseries.com/eFax/incoming/5442.ZIP
hxxp://www.recordsmanagementservices.com/eFax/incoming/150721/5442.ZIP
hxxp://files.counseling.org/eFax/incoming/150721/5442.ZIP