CALLISTO GROUP

TLP: White

F-Secure

SUMMARY

The Callisto Group is an advanced threat actor whose known targets include military personnel, government officials, think tanks, and journalists in Europe and the South Caucasus. Their primary interest appears to be gathering intelligence related to foreign and security policy in the Eastern Europe and South Caucasus regions.

In October 2015 the Callisto Group targeted a handful of individuals with phishing emails that attempted to obtain the target's webmail credentials.

In early 2016 the Callisto Group began sending highly targeted spear phishing emails with malicious attachments that contained, as their final payload, the "Scout" malware tool from the HackingTeam RCS Galileo platform.

These spear phishing emails were crafted to appear highly convincing, including being sent from legitimate email accounts suspected to have been previously compromised by the Callisto Group via credential phishing.

The Callisto Group has been active at least since late 2015 and continues to be so, including continuing to set up new phishing infrastructure every week.

F-SECURE LABS
THREAT INTELLIGENCE

Malware analysis
Whitepaper

Published: April 2017

CONTENTS

INTELLIGENCE

INTRODUCTION

The **Callisto Group** is an advanced threat actor that, as far as we know, has never been identified. The primary focus of the **Callisto Group** appears to be intelligence gathering related to European foreign and security policy.

This report focuses on describing activity dating from late 2015 to the present day that we have been able to definitively associate with the **Callisto Group**. Also, some indications of loosely linked activity dating back to at least 2013 is provided in the section "Related activity" (page 3). However, we do not currently attribute this older activity directly to the **Callisto Group**.

ATTACK OVERVIEW

PHASE 1: CREDENTIAL PHISHING

In October 2015, the **Callisto Group** was observed sending targeted credential phishing emails with the subject "Remove account [target's Gmail address]". These emails purported to come from Google alerting the target that their Gmail account was about to be removed. The emails requested the target to click a link to prevent their account from being removed. If clicked, this link would lead to a phishing website that attempts to harvest the target's Gmail credentials.

The emails were designed to appear authentic and convincing. The domains used Google or commonly known Google services in both the referenced links and the sender's email.

Based on our information, these emails were highly targeted and were only sent to a handful of targets. At least some of the recipient Gmail addresses were personal accounts of the target and not readily available to the public, suggesting thorough reconnaissance by the attackers.

Known targets include European military personnel. We also have reason to believe this or related phishing incidents targeted key personnel in European think tanks.

PHASE 2: SPEAR PHISHING WITH MALICIOUS ATTACHMENTS

In early 2016, the **Callisto Group** was observed sending targeted spear phishing emails containing malicious attachments. These emails were sent from email accounts of individuals likely to be familiar to the recipient. We believe these email accounts were compromised in the previous phase of the attack, or in similar related phishing attacks.

Known spear phishing emails made reference to a conference with relevance to European security policy. The malicious attachments purported to be invitations or drafts of the agenda for the conference. The compromised email accounts used to send the spear phishing emails belonged to individuals involved in organizing the conference. Combining this information together resulted in highly convincing spear phishing.

Known targets of these spear phishing emails with malicious attachments include military personnel, government officials, think tanks, and journalists in Europe and the South Caucasus. We are currently not aware of any evidence suggesting any of these individuals were compromised, just that they were targeted.

All known malicious attachments sent with these spear phishing emails were Microsoft Word .docx files. None of the known files exploited any vulnerabilities. Rather, the files utilize a feature of Microsoft Word that allows "objects" to be embedded in docx files. In the case of these malicious files, the embedded object is the malware executable.

IMAGE 1
Icon for an embedded malware executable in a malicious attachment

IMAGE 2
Icon for an embedded malware executable in another malicious attachment

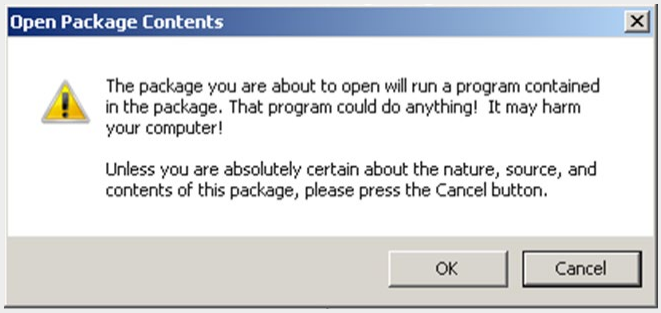

IMAGE 3
Warning prompt shown to the user by recent versions of Microsoft Word if the user clicks the icon for the embedded malware executable. The malware will only be executed if the user clicks "OK".

For the embedded malware to be executed, a user needs to click an icon in the docx file (see Images 1 and 2 for examples). Additionally, in recent versions of Microsoft Word, if a user clicks the icon for the embedded executable, Word will prompt the user with a warning (see Image 3). The payload will only be executed if the user acknowledges the prompt.

MALWARE USAGE

In all known malicious attachments, the final payload was a variant of the "Scout" tool from the HackingTeam Remote Control System (RCS) Galileo hacking platform. HackingTeam is an Italian software company that created RCS, which they describe as "the hacking suite for governmental interception".[1] In July 2015, news emerged that HackingTeam had been breached. One of the consequences of this incident was the then latest version of RCS Galileo being leaked to the public.[2]

As a result of the leak, both the source code and the ready-made installers for the RCS platform were made available for anyone to use. Based on our analysis of **Callisto Group**'s usage of RCS Galileo, we believe the **Callisto Group** did not utilize the leaked RCS Galileo source code, but rather used the leaked ready-made installers to set up their own installation of the RCS Galileo platform. The process for using the leaked installers to set up an RCS Galileo installation has been described online in publicly available blogposts, making the process trivial to achieve.

In the known spear phishing attacks by the **Callisto Group**, they employed the "Scout" malware tool from the RCS Galileo platform. The "Scout" malware tool is a light backdoor intended to be used as an initial reconnaissance tool to gather basic system information and screenshots from a compromised computer, as well as enable the installation of additional malware.

1. HackingTeam; http://www.hackingteam.it/
2. Arstechnica; *Hacking Team gets hacked; invoices suggest spyware sold to repressive govts*; published 7 Jul 2015; http://arstechnica.com/security/2015/07/hacking-team-gets-hacked-invoices-show-spyware-sold-to-repressive-govts/

CONSEQUENCES

If a target of the credential phishing described in "Phase 1: credential phishing" clicked a link in the email and proceeded to input their email credentials on the resulting phishing website, this would provide the **Callisto Group** with the target's email credentials. Unless the target was using two-factor-authentication, the **Callisto Group** would then have full access to the target's email account.

We are confident the **Callisto Group** used this type of access to a target's email account for the purposes of sending spear phishing to other targets. We also believe it is highly likely that the **Callisto Group** would leverage the same access to read and monitor the target's email activity.

If a target of the spear phishing described in "Phase 2: malware deployment" opened the email attachment and, crucially, clicked on the icon in the attachment, this would lead to the target's computer becoming infected with the "Scout" malware tool from the RCS Galileo platform. This malware tool would have gathered basic information on the target's computer and delivered these to the **Callisto Group**. This malware tool would have also enabled the **Callisto Group** to install additional malware on the target's computer.

In effect, this would have provided the **Callisto Group** with full remote access to the target's computer, and by extension, to any data accessible to the target via their computer.

TARGETING AND ATTRIBUTION

The most obvious common theme between all known targets of the **Callisto Group** is an involvement in European foreign and security policy, whether as a military or government official, being employed by a think tank, or working as a journalist. More specifically, many of the known targets have a clear relation to foreign and security policy involving both Eastern Europe and the South Caucasus.

This targeting suggests the **Callisto Group** is interested in intelligence gathering related to foreign and security policy. Furthermore, we are unaware of any targeting in the described attacks that would suggest a financial motive.

It is worth noting that during our investigation we uncovered links between infrastructure associated with the **Callisto Group** and infrastructure used to host online stores selling controlled substances. While we don't yet know enough to fully understand the nature of these links, they do suggest the existence of connections between the **Callisto Group** and criminal actors.

While the targeting would suggest that the main benefactor of the **Callisto Group**'s activity is a nation state with specific interest in the Eastern Europe and South Caucasus regions, the link to infrastructure used for the sale of controlled substances hints at the involvement of a criminal element. Finally, the infrastructure associated with the **Callisto Group** and related infrastructure contain links to at least Russia, Ukraine, and China in both the content hosted on the infrastructure, and in WHOIS information associated with the infrastructure.

It is possible to come up with a number of plausible theories to explain the above findings. For example, a cyber crime group with ties to a nation state, such as acting on behalf of or for the benefit of a government agency, is one potential explanation. However, we do not believe it is possible to make any definitive assertions regarding the nature or affiliation of the **Callisto Group** based on the currently available information.

CONTINUING ACTIVITY

The **Callisto Group** continues to be active. While they have been last known to employ malware in February 2016, they continue setting up new phishing infrastructure every week.

Should the **Callisto Group** be alerted to the fact that they have been noticed, we do not know how they will react. They may stop everything or they may continue as if nothing has happened. However, as long as they believe they are succeeding in staying unnoticed, we believe it is highly likely that they will continue their phishing activity, and follow up any successful compromises with additional malware attacks.

IDENTIFICATION, MITIGATION, AND REMEDIATION

IDENTIFYING CALLISTO GROUP ACTIVITY

Appendix A provides indicators of compromise that can be used to attempt to identify **Callisto Group** activity. Every effort has been made to thoroughly document the tools, techniques, and procedures of the **Callisto Group**, as well as possible methods of identifying whether an individual or organization has been targeted or compromised by this threat actor. However, it is possible that the **Callisto Group** is also using other tools, techniques, and/or procedures that would evade identification by the provided methods.

It is highly encouraged that any, even slight, suspicion of compromise be thoroughly investigated.

MITIGATION AGAINST CREDENTIAL PHISHING

Using two-factor authentication for accessing email would prevent the attackers from using compromised credentials to gain access to a target's email account. However, the compromise of login credentials, especially should the victim not employ proper password hygiene (such as by reusing passwords), is a security risk in itself.

REMEDIATION AGAINST CREDENTIAL PHISHING

Should a user suspect having fallen victim to credential phishing, immediate remediating action should be taken to reset the suspected compromised credentials and enable two-factor authentication. Any other services where the user may have reused the same username and/or password should also have the credentials reset.

These immediate actions should be followed by a thorough investigation to determine the extent of the possible compromise, to understand what data may have been compromised, what actions the attackers may have taken with the help of the compromised credentials, and what the implications of these actions and compromise may be.

MITIGATION AGAINST SPEAR PHISHING AND RCS GALILEO

The spear phishing emails used in the known attacks by the **Callisto Group** were so convincing that even skilled and alert users would likely have attempted to open the malicious attachment. However, simply viewing the attachment would not have resulted in an infection as the document did not attempt to exploit any vulnerabilities.

Actual infection would have required the user to attempt to click a specific icon in the opened attachment. Furthermore, at least recent versions of Microsoft Word will prompt the user with an additional warning stating that what the user is about to do is dangerous. For the infection to succeed, the user would either have to acknowledge the prompt or be using an old enough version of Microsoft Word to not be warned.

Additionally, the malware payload used, RCS Galileo, is relatively well known. Therefore, most antivirus solutions provide good protection against RCS Galileo and would have blocked the execution of the malware payload. Using an up-to-date antivirus solution with all protection features enabled is the most effective mitigation against highly targeted attacks such as these.

REMEDIATION AGAINST RCS GALILEO

Should a user suspect having become infected with RCS Galileo, their computer should immediately be disconnected from the internet. However, care should be taken to not power off the computer as this would hinder the ensuing investigation into the compromise.

Once the computer has been disconnected from the internet, the malware will be unable to communicate with its command and control server, thereby disrupting the attacker's ability to control the computer. This should immediately be followed by initiating a thorough forensic investigation into the compromise.

Should the affected organization or individual not have complete confidence in their ability to properly perform such an investigation, they should employ outside assistance.

APPENDIX A | INDICATORS OF COMPROMISE

SAMPLE HASHES

SHA1 of related RCS Galileo sample. We believe other similar samples exist.

07cdc67d211d175cd9d418dc5482b3f17d93526a

DETECTION NAMES

F-Secure detects **Callisto Group** activity with a variety of generic, behavioral, and other detections including the following:

Gen:Variant.Symmi.54992

FILE PATHS

Upon infection, known samples of **Callisto Group**'s RCS Galileo have stored copies of themselves in the following locations:

%TEMP%\Microsoft Word.exe
%TEMP%\WinWord.exe
>startup folder<\bleachbit.exe
>startup folder<\BluetoothView.exe

COMMAND & CONTROL INFRASTRUCTURE

Known command & control servers

89.46.102.43

PHISHING INFRASTRUCTURE

Domains known or believed to be used in relation to phishing. These may be used as targets of links or as domains for sender email addresses.

accounts-google.eu
accounts-mail.asia
authentification-request.top
auth-login.top
drive-login.com
drive-meet-goodle.ru
emailapp.pw
fco-gov.pw
fco-net.pw
google-accounts.eu
google-plus.top
google-service.eu
go-veryfication.link
hotmail-online.eu
icloud-service.pw
live-com.pw
live-login.info
login-access.top
login-live.review
login-livecom.in
login-livecom.info
login-live-com.pw
misrcosofts.com
node005-prevention-aol.link
node03-prevention-icloud.link
platforma.link
prevention-aol.link
prevention-aol.top
prevention-icloud.link
qooqle-support-mail.pw
screenname.click
screenname-aol.pw
secure-lcloud.accountant
secure-store-lcloud.top
service-mail.asia
service-mail.in
serv-login-com.pw
shared-docs.pw
store-icloud.link
support-gmail.pw
support-mail.pw
support-mail.top
updatemail.in
yahoocentermail.info
yahoocentermail.pw
yahoomailfree.pw


F-Secure