# comprehensive profile of Carbanak activity in 2016/17

January 18, 2017 | 5 minutes read | SpiderLabs Researcher

The Trustwave SpiderLabs team has been actively tracking a malicious campaign conducted by the well-known Carbanak Cybercrime group for the latter part of 2016 and into 2017. Carbanak is one of the most prolific organized Russian cybercrime groups and is responsible for the theft of billions of

dollars from legitimate economies to the criminal underground. Malware attributed to this group has been cited in the infamous "billion dollar bank hack" of 2015 and the massive Oracle/Micros hack of mid-2016 that led to over a million vulnerable POS servers. Carbanak malware (Carberp family) was also cited by Homeland Security and the FBI as an Indicator of Compromise for Russian Intelligence Service malicious activity in their most recent report GRIZZLY STEPPE – Russian Malicious Cyber Activity.

Trustwave has tracked Carbanak activity in the latter half of 2016 and found them to be targeting hospitality and retail victims in Europe and North America, specifically targeting their internal corporate secrets and protected payment card data. Trustwave published a blog earlier in the year within initial findings but has now released the complete malicious campaign profile in a 45-page Advanced Threat Report. The blog post below is a summary of the malicious profile we have developed for this actor.

## Operation Grand Mars

During September and October of 2016, Trustwave SpiderLabs was simultaneously consulted by several leading organizations from the hospitality sector in Europe and the United States to analyze suspicious and potentially malicious activity on their network including servers, point of sale terminals, and client workstations spread across different properties and locations.

The motivation of this operation appears to be financial gain, total control of the infrastructure and collection of bots within the victim organizations. During the forensics investigation and analysis, we were given the impression that several activities have been performed by different persons or even different groups of people. We believe that malicious gangs cooperated in this operation with each group holding their own role and task. It soon became obvious that we are dealing with organized crime responsible for establishing this complex system of network hosts and large number of malicious files in order to perform the attacks against multiple victims.

The organizations under attack were first alerted either because their enterprise AV service discovered pieces of potentially malicious software or from suspicious indicators in Windows event logs. Since the victims were different organizations the investigations were held by separate teams within Trustwave but intelligence sharing among the teams proved that several similarities existed among the attacks.

## Entry Point

The common successful entry point within all operations was an email message targeted to victim's public-facing services that contained a Microsoft Word document attachment. Upon opening the attachment multiple malicious files were created or downloaded allowing the attackers to gain some level of access into the victim's infrastructure. In some cases,

attackers actually called the victims over the phone, social engineering vector, in order to trick staff into opening the attachment.

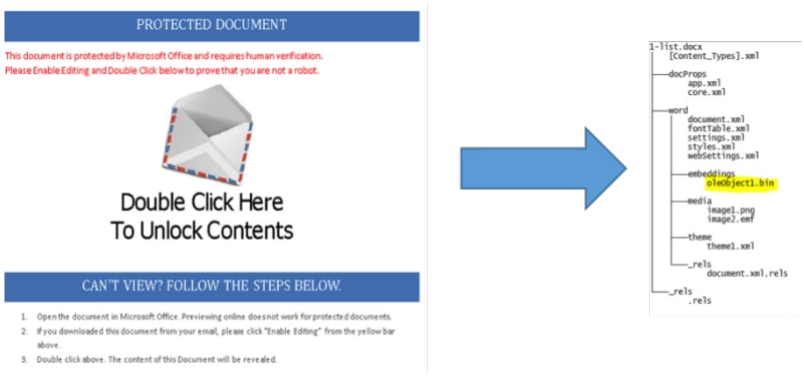


***Figure 1**: Malicious Word document*

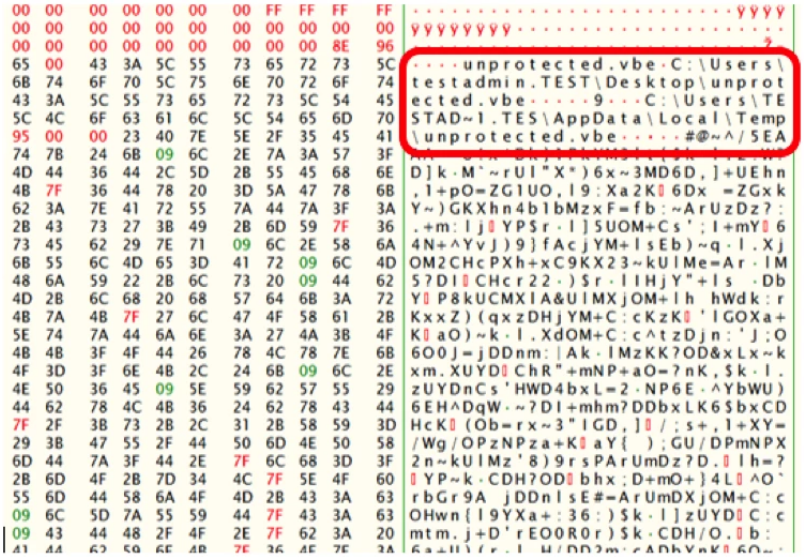


***Figure 2**: Encrypted Script from malicious document*

So the malicious Word document when opened, executes the embedded script and drops the following four files:

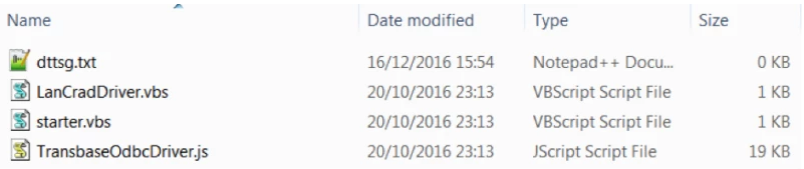


***Figure 3**: Files dropped on execution of embedded VBE script*

## Malicious Scripts

The role of each of the four dropped files is visually represented in the following activity diagram:

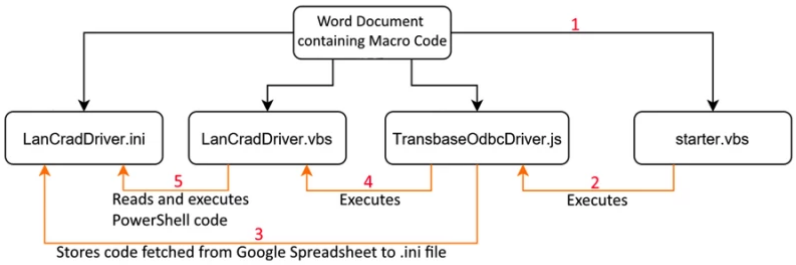


***Figure 4**: File process*

## Pastebin Account

An additional file "dttsg.txt" has the following structure and is split into two sections "last" and "code" providing another covert channel during this operation.

{last: "abc123", code: "ZGltIHh4eA=="}

*Code from Pastebin*

Contents of this file retrieved from a Pastebin account used in the attacks as part of the command control mechanism by the attackers belongs to an individual identified as "Shtokov". This is yet another (weak) indication of the involvement of Russian/Eastern European actors in these attacks.

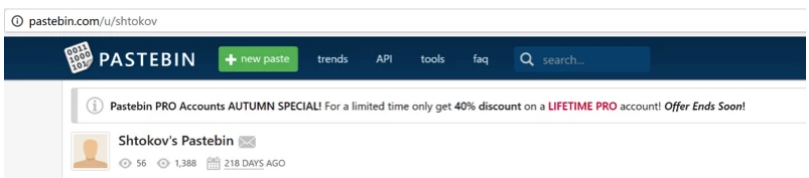


***Figure 5**: Shtokov Pastebin site used in Command and*

*Control*

Data from section "last" is written into registry perhaps to keep track of last executed command and "code" which is Base64 encoded used as an argument and allows attackers to execute one of the following commands "Destroy", "GetCompInfo", "GetProcList" and "RunCMDLine" as displayed below. However, usage of this feature was not observed during our investigation.

```
var cod_data =
Base64.decode(cmb_ob.c);
if(cod_data == "#deleteBot#"){
destroy();
}else if(cod_data ==
"#GetCompInfo#"){
Log("$stdOut$" +
GetComputerInform());
}else if(cod_data ==
"#GetProcList#"){
Log("$stdOut$" +
GetCompProcess());

}else if(
cod_data.indexOf("#RunCMDLine#
") !== -1){
var cmd_str =
split(cod_data,'#RunCMDLine#',
2);
Log("$stdOut$" +
RunCMDLine(cmd_str[1]));
}else{
```

```
var tempname1 =
"LanCradDriver.ini";
var tempname2 =
"LanCradDriver.vbs";
var tmpPath = GLBFolderPlus;
var tempath1 = tmpPath +
"\\"+tempname1;
var tempath2 = tmpPath +
"\\"+tempname2;

var f =
FSO.OpenTextFile(tempath1,2,fa
lse,-1);
f.Write(cod_data);
f.Close();
```

*Arguments from Pastebin*

## Privilege escalation

Privilege escalation was performed by means of various Pass-the-Hash techniques while persistence was achieved by utilizing scheduled tasks and several of the Operating System's auto-start locations. Ultimately these actions allowed attackers to gain Domain or even Enterprise Admin access and gain network access by using several resources as Command & Control points in Europe and the US.

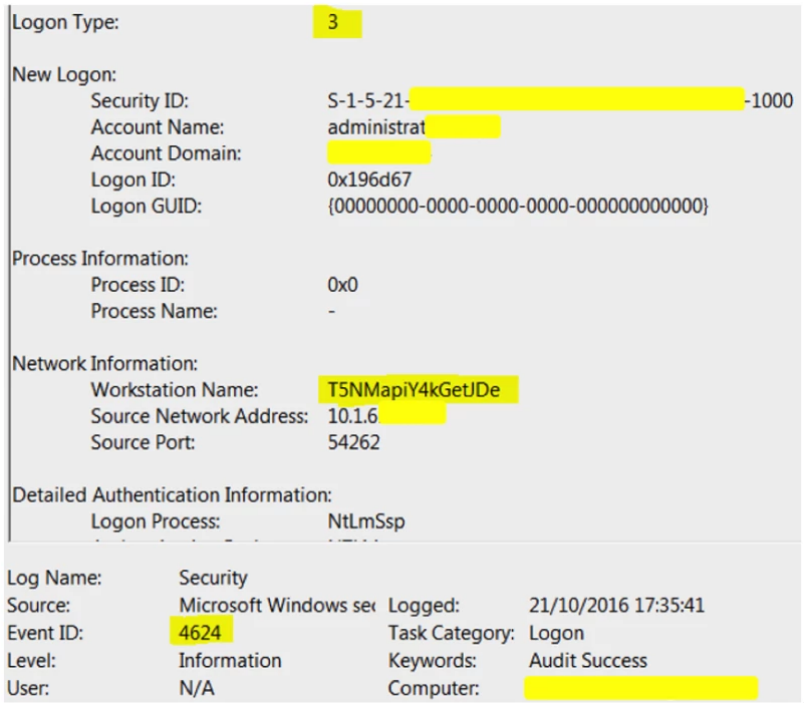


***Figure 6**: Event log showing Pass-the-Hash indicators*

An event ID 4624 displayed above showing the usage of a local account performing network logon (Logon Type:3) using a randomized source computer name (Workstation Name: T5NMapiY4kGetJDe) most probably a result of an automated tool.

## Google Docs

Cloud services such as Google Docs and Google Forms were involved allowing attackers to keep track of infected systems, spread malware and perform further malicious activities. Usage of such services as part of the attack is always beneficial for attackers since most enterprise networks allow access to these and it is almost impossible to blacklist them.

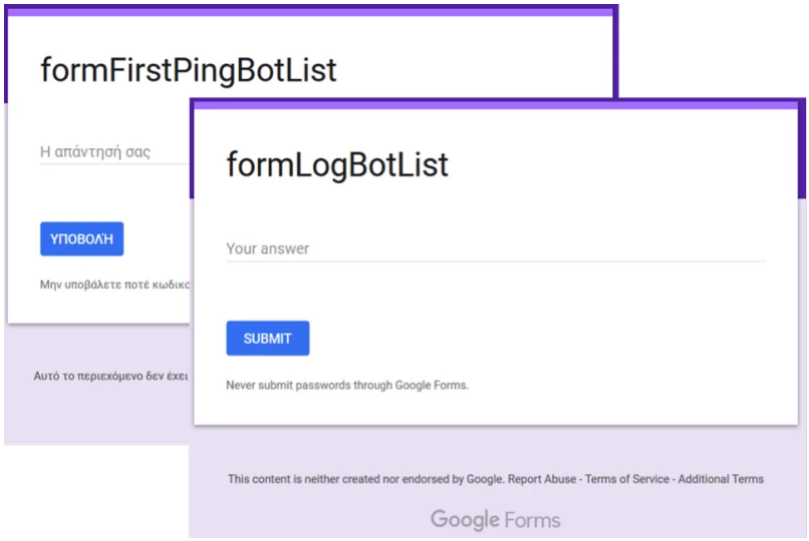


***Figure 7**: Google forms used for tracking victims*

Malicious code used in these operations was split among memory resident code, scripting code (PowerShell, JavaScript, VBS), executables (often variants of existing malware) and finally usage of customized versions of toolkits such as Metasploit, PowerSploit and Veil Framework.

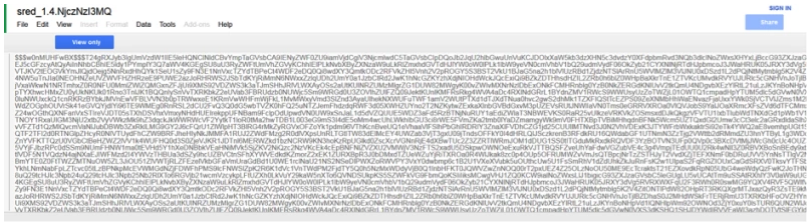


***Figure 8**: Encoded PowerShell commands retrieved from Google Spreadsheet*

## Anunak variant and other signed malware

What seems to be the core tools of these activities is a variant of Anunak, remote backdoor, along with a Visual Basic Script specially crafted with data exfiltration features.

One other significant finding is that some of the executables were signed using valid certificates from Comodo, a Certification Authority. Based on the analysis of the certificates we believe that the attackers actually used fake identity and purchased these to bypass further security controls potentially in place.

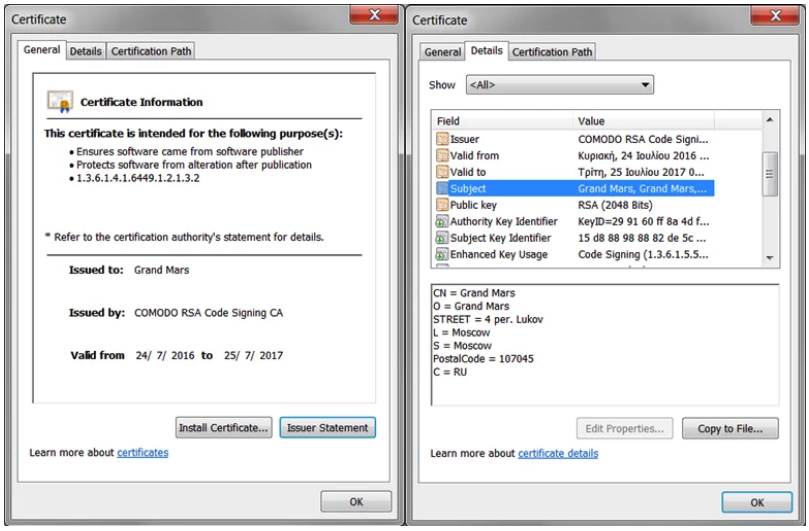


***Figure 9**: Certificate used to code-sign Anunak*

## Threat Report

We called this operation "Grand Mars" after the company name that cyber criminals used in one of the digital certificates purchased from Comodo. Most likely, the name and all Russian details (city, address etc.) used in the certificate details are fake, however, the point that someone actually paid for these is a strong indicator that we are dealing with organized criminal activities.

This threat report describes what we believe to be a systematic criminal operation of attacks targeting the hospitality sector in

Europe and the US, at least at this time. However, the findings suggest that other sectors such as e-commerce and retail are equally at risk and the campaign could just as easily spread to other parts of the world.

The majority of IP addresses used as Command & Control points were unknown systems located within Europe (UK, France, Sweden etc.) indicating that attackers were trying to bypass network security controls by using seemingly innocuous servers as malicious endpoints. During the investigation of this operation we monitored access to these C&C servers and found that the attackers would occasionally change their C&C server and take the previous one off-line. We believe that this alternating use of C&C servers was a purposeful action by attackers in order to remain as stealthy as possible. Their location and role is depicted below in the European region map. (note: Three servers located in N. America, not shown for simplicity).

This threat report intends to provide an analysis of this operation and document:

- Our analysis and findings in a way that describe the nature of malicious activities, the tactics and tradecraft utilized by the attackers, possible motives and the attribution of the threat actors behind these attacks.
- Remediation actions and advice to organizations that have already been targeted by this campaign of attacks or willing to take proactive

countermeasures.
- Indicators of Compromise (IOCs) that will benefit organizations seeking to either undertake a compromise assessment on their own (or with the help of a team that specializes in threat hunting and compromise assessments such as Trustwave SpiderLabs), or to proactively put in place detection mechanisms for providing an early warning system if and when the organization is targeted.

However, it must be noted that this threat report does not and is not capable of replacing formal incident response actions and procedures that must be undertaken to mitigate the threat and restore business functions as per the Organizational Incident Response/Disaster Recovery roadmap.

Thanks to Sachin Deodhar and Rodel Mendrez for their contribution to the research described in this post.

**UPDATE**: Here are the SHA1 fingerprints of the two certificates found in this investigation:

c1:9c:df:78:e2:34:29:fa:f6:86:bd:f8:ff:dc:f5:ef:0b:9f:14:56
aa:a6:e7:dc:9b:df:2d:90:31:c0:ec:b0:32:bc:68:67:77:20:5f:92

# Latest SpiderLabs Blogs