Wolf in Sheep’s Clothing
- Undressed
Virus Bulletin 2018

www.csis.dk
Wolf in Sheep’s Clothing
- Undressed

Who’s who:

- Aleksejs Kuprins
- Benoit Ancel
Wolf in Sheep’s Clothing
- Undressed

What to expect

1.00 Introduction
2.00 Win32.Agent
3.00 Android.Agent
4.00 IOS.Agent
5.00 Multi-platform-malware
6.00 [SPOILERS REDACTED]
7.00 Victims intelligence
8.00 Toolset
Wolf in Sheep’s Clothing
- Undressed

1.00  
Introduction
Origin of the research

Investigation around VPS used for phishing, banking...

- **1226** domains resolved
- **1** really interesting
• Fake Google Play page acting as dropzone.

• Payloads are selected depending on the User-Agent of the victim:
  • if ( /iPhone|iPad|iPod/i.test(navigator.userAgent))
    • i.diawi.com/i3cuz6 (IPA)
  • else if ( /Android/i.test(navigator.userAgent))
    • update.apk
  • else:
    • Update.exe

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td></td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>chrome.apk</td>
<td>2018-06-26 06:13</td>
<td>12M</td>
<td></td>
</tr>
<tr>
<td>m5.exe</td>
<td>2018-04-13 02:50</td>
<td>1.4M</td>
<td></td>
</tr>
<tr>
<td>ssh.apk</td>
<td>2018-03-20 23:04</td>
<td>11M</td>
<td></td>
</tr>
<tr>
<td>update.apk</td>
<td>2018-06-19 04:31</td>
<td>12M</td>
<td></td>
</tr>
<tr>
<td>update.exe</td>
<td>2018-06-26 01:29</td>
<td>1.3M</td>
<td></td>
</tr>
<tr>
<td>update1.apk</td>
<td>2018-06-18 10:01</td>
<td>12M</td>
<td></td>
</tr>
<tr>
<td>update_m5wali.exe</td>
<td>2018-03-23 04:56</td>
<td>1.4M</td>
<td></td>
</tr>
<tr>
<td>update_old.apk</td>
<td>2018-03-22 19:08</td>
<td>12M</td>
<td></td>
</tr>
</tbody>
</table>
Wolf in Sheep’s Clothing
- Undressed

2.00
Win32.Agent
Win32.Agent

- Update.exe is a RAT for Windows (probably a debug build)
  - The malware is composed of 2 stages:
    - 1- Loader
    - 2- RAT
  - Already on VT with good detections
Win32.Agent.W1_RAT

~ 20 features available, nothing advanced or fancy:

| Feature                        | File Operations         | Utilities          | Services          | Administration | Network | \---
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint victim</td>
<td>Read file</td>
<td>Rename file</td>
<td>List processes</td>
<td>exec</td>
<td>Screencast</td>
</tr>
<tr>
<td>Search files</td>
<td>Is</td>
<td>Delete file</td>
<td>Kill process</td>
<td>Get keylogger logs</td>
<td>Mic</td>
</tr>
<tr>
<td>Upload file</td>
<td>Copy file</td>
<td>Create dir</td>
<td>Enum services</td>
<td>Credentials stealers</td>
<td></td>
</tr>
<tr>
<td>Get file size</td>
<td>Move file</td>
<td>Edit timestamp file</td>
<td>Stop service</td>
<td>Autokill</td>
<td></td>
</tr>
</tbody>
</table>

- \[Image of a table depicting various features of Win32.Agent.W1_RAT\]
Wolf in Sheep’s Clothing
- Undressed

3.00
Android.Agent
Android.Agent

• Not packed (probably debug build)

• Looks like basic android RAT
Android.Agent

• Patchwork of old codes:
  • https://github.com/koush/Screenshot (9yo)
  • https://github.com/murali129/ScreenOCR (1yo)
  • https://github.com/jakubkinst/DEECo-Offload (3yo)
Wolf in Sheep’s Clothing
- Undressed

4.00
IOS.Agent
IOS.Agent

• Copy paste from:
  • https://github.com/andrealufino/ALSystemUtilities (no longer maintained, 3yo)
  • https://github.com/gali8/Tesseract-OCR-iOS
  • https://github.com/davidmurray/ios-reversed-headers

• Broken application
  • Alpha ?
Wolf in Sheep’s Clothing
- Undressed

5.00
Multi-platform malware
Multi-platform malware

- It looks like somebody tried to have a multi-platform tool
- Lame code (copy paste, bugs, scam app (ios))
- Lame infrastructure

- It looks like an audacious cybercrime actor is trying something.
Aaahh... Panels!

Unknown panels located on the same domain, used as **C&C** for mobile malware
Aaahh... Panels!

Panels entirely open with full backup of databases and all stolen data.
Data!

• It’s \( \sim 20 \text{ Gb} \) of data available
  • Pictures
  • Audio records
  • Documents
  • Smartphone configuration
  • Everything stolen is available in the databases
After a quick analysis it’s clear, this actor is interesting.
Wolf in Sheep’s Clothing
- Undressed

6.00
Kumar Manish, WOLF and the pack
Kumar Manish
CEO of Wolf Research

- All the data point to a man: Kumar Manish from Wolf Research.
- Fun fact: opendir « website_logo » on the malware C&C with Wolf Research

Logo and Kumar Manish Picture
Kumar Manish
CEO of Wolf Research

NO KIDDING!
Wolf Research develops advanced big data systems, cyber security & AI, and data extraction solutions for the government and homeland security sectors.

HQ in Germany, offices in: Cyprus, Bulgaria, Romania, India and (possibly) US
Wolf Research

Known stories:

• Motherboard: The Forgotten Prisoner of a Spyware Deal Gone Wrong
  (Scam attempt against Mauritania Government)
• Forbes: Meet The 'Cowboys Of Creepware' -- Selling Government-Grade
  Surveillance To Spy On Your Spouse (spouseware business)
• Bloomberg: The Post-Snowden Cyber Arms Hustle
• Hacking Team emails leak

*The company's co-founder Manish Kumar is a "criminal of the worst kind,"
according to David Vincenzetti, the CEO of Hacking Team*
• Approximate transcription:

• “My developers are based in Romania at the moment. I am doing all my development in Romania. In Puna, in India I have develo... Sorry, the TESTING team. Testing. Testers. They are testers, MKAY? So, in India, I don’t do any developments, only testing. And these are my own cousins, you know, like my family, guys and... Because I need trusted people, I cannot give them the payload and they make a mistake, copy, you know and integrity is very important. I need to maintain the team. So, its very important, so...”
Wolf Research – leader of the pack

Sub contractors:

Development based in Romania (Decode.ro)

Testers in India (Puna) (Squarebits)
This name appears everywhere: **Iurie Gutu**

- One of developers of IOS/Android malware (with Valentin Brad)
- The apk/ipa malware is invoiced to a Romanian Company: **Decode.ro**
Dev - Decode.ro
Panel and IOS developments

commit 1c594f94b3842d9b0787f22310d6a7a151cd804
Author: Iurie <iurie.gutu@decode.ro>
Date: Tue Jun 19 18:17:04 2018 +0000

device status
commit 709c4bc7d79bff5e3bca886f3febc877caae24b
Author: Iurie <iurie.gutu@decode.ro>
Date: Wed Jun 6 09:11:23 2018 +0000

screen recording and ocr separately work
commit 2f04a4d6051b01fc85ab818c99072becc2e4a515
Author: Iurie <iurie.gutu@decode.ro>
Date: Mon Apr 2 07:41:43 2018 +0000

wording change
commit 654b54a5b5442e26abf80ac4622026098ed7b8f
Author: Iurie <iurie.gutu@decode.ro>
Date: Mon Apr 2 07:23:52 2018 +0000

css fixes
commit 2eb756ec0c5ef74daa56a3794ed1af4b60df3194
Author: Iurie <iurie.gutu@decode.ro>
Date: Fri Mar 30 14:48:54 2018 +0000

pic

<string>only manish kb</string>

<string>ProvisionedDevices</string>

<string>decode.ro</string>
Squarebits

Mobile App Development Company based in India

Innovative Mobile App Development Company

When you wish to take your business to the next level by gaining consumer attention & better presence with robust gaming & mobile apps, We, at Square Bits, are here to help you with our mobile applications development services.
Squarebits

Google drive link found in the database:
Squarebits
THE KUMAR FAMILY
Wolf in Sheep’s Clothing
- Undressed

7.00
Victims intelligence
Victims intelligence

A true globetrotter

Public IPs based geolocation for the smartphone
Victims intelligence

- Looks like demo smartphone for sellers
- Different actors testing or presenting Wolf Research products
• Key quotes:
  • “You find your targets, you exploit them and after that you can use this kind of system to complete your investigation and have all the information you need”
  • “- We stay in touch? – Yes, if you need another meeting “
  • “This is a test for a customer”
• “This is a test for our customer, how are you? Good? [...] It’s not too long this morning?”
• Many calls/SMS from +336 numbers (France, mobile phone) in the database
• **French audio records**
• 90.102.1.97 used by the smartphone (registrant rlh@nexatech.fr)
• SMS in the database:
  
  « DHL EXPRESS from NEXA TECHNOLOGI is scheduled for delivery TODAY by End of Day. Track at ... »
• A strange apk called « **Nexa Tracker** »
• Personal phone number used by a **Nexa VIP**
• Key quote:
  • “Allo, oui bien sur, ça va ? […] Je me parle tout seul”
  • “Hi, how are you ? I’m just talking to myself”
• **Interesting connection:**
  • Can be an attack vector
  • (Very) Big company in WIFI interception

• **Interesting data**
  • You don’t see WiSpear tools every days 😊

• **Proof:**
  • Smartphone named “Wispear”
  • Geolocation
  • Pictures
WiSpear
WiSpear
“Prosafe is a leading owner and operator of semi-submersible accommodation, safety and support vessels.”

A lot of pictures of the Prosafe HQ in Cyprus
Partnership

Wolf Research

The panels

Nexa
Amesys

WiSpear

Prosafe

Political targets

...
Wolf in Sheep’s Clothing
- Undressed

8.00
Toolset
The testing phone

Test smartphones contain a lot of useful internal data:
The testing phone
The W1 Crypter

Download W1 Crypter.rar - UpmyBit
www.upmybit.com/ftp/XNo → Traduire cette page
begin
    FillChar(SI, SizeOf(TStartupInfoW), #0);
    FillChar(PI, SizeOf(TProcessInformation), #0);
    SI.cb := SizeOf(TStartupInfoW);

    // This is the trick, right here!
    // CreateProcessW doesn't get detected by most AVs
    // Because wide versions of this trick aren't common.
    if CreateProcessW(PWideChar(WideString(FilePath)), PWideChar(WideString(Parameters)), nil, nil, FALSE, CREATE_SUSPENDED, nil, nil, SI, PI) then
      begin
        CT := Get4ByteAlignedContext(CTBase);
      end;
The W1 Crypter

<table>
<thead>
<tr>
<th>Anti Virus</th>
<th>Clean</th>
<th>Not Clean</th>
<th>PRE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avast</td>
<td>☑</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avg</td>
<td>☑</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avira</td>
<td>☑</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AhnLab V3</td>
<td>☑</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Baidu</td>
<td></td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>E-Scan</td>
<td></td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>Malware Bytes</td>
<td></td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>360 Total Security</td>
<td>☑</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KingSoft</td>
<td></td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>Comodo</td>
<td>☑</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kaspersky</td>
<td></td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>Smadav</td>
<td></td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>Panda</td>
<td>☑</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KG2 Total</td>
<td>☑</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft</td>
<td></td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>WebRoot</td>
<td></td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>Nano Antivirus</td>
<td></td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>Mcafee</td>
<td>☑</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eset Nod 32</td>
<td>☑</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bitdefender</td>
<td>☑</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Norton</td>
<td>☑</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DrWeb</td>
<td></td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>TentCent</td>
<td></td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>HouseCall</td>
<td></td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>VBA32</td>
<td>☑</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virebot</td>
<td>☑</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F-Prot</td>
<td>☑</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preventon</td>
<td>☑</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SuperAntiSpyware</td>
<td></td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>Quick Heal</td>
<td></td>
<td>☑</td>
<td></td>
</tr>
</tbody>
</table>
Attack vectors (?)
• Key quotes:

• “- The target would get suspicious. What do you need to control?”
  “- I need to turn on this functionality”
  “- No-no-no, we are not rooting or jailbreaking. If you don’t root or jailbreak
you cannot go any deeper, you cannot turn on or off…”
  “- Мы не джэйлбрэйкаем это дело.” (1st RU speaker: “We aren’t jailbreaking
this.”)
  “- Поэтому мы не можем [сообщения вывезти].” (2nd RU speaker: “That’s
why we cannot extract the messages.”)
  “- We can do only if we use 0 days.”
• Key quote:
  • “- Actually, we are using Google. Everyone does Google, [no one test the apps]”
    “- This is why we like this solution”
    “- Even Anti-Virus wouldn’t get it if it’s from the Google App Play store – it will bypass”
    “- All these years we always wanted to go into the market of phone penetration, but it always was based on Trojan horses and we didn’t want to be in this boat until we found this solution, so we integrated it, because this is something....”
MISC

- Audio records
• Key quotes:
  “- We prefer not to work with opposition guy.”
  “- We are not sure about this. Same as Bangladesh.”
  “- Because when they will loose the election, they will publish the blog, they will publish something in the news, we will be discovered somehow, we afraid of this stuff. So we never work with opposition, never. We always work with the leader.”
• Key quotes:
  - “Although there are some Israeli companies that sold anything [everything?] [0days?] But as far as I know, they don’t have the budget to spend on it”
  - “They have it my friend they have it”
  - Only for you”
  - [laughs]
• Key quotes:
  • “[???] start to **South America**, start in about 30 million. I’m here since 8am.”
    - Really?
    - Since 8, I’m in the meetings here.
    - Really? How many meetings you are attending? Three-four?
    - It’s the second. Just the first one was like yesterday [???] TalkTalk. Until March 20 it’s talking.
• Approximate transcription:
  - “I’ve been to Egypt and we’ve done the same product. Also Linux, Mac, Windows. Same way, with exploits.”
  - “It was good?”
  - “We had it in 2015. Now we are still going for service from time to time, every year we have to go…”
Conclusion

• Only the tip of the iceberg
• This kind of behavior can do great damage to international operations
  • Wolf Research: Bad legit company or good scammers?
  • Who is currently regulating the spyware business?
Thank you

For more information, please contact
pkr@csis.dk

www.csis.dk