Operation Buhtrap

Jean-Ian Boutin, Anton Cherepanov, Jan Matušík
AVAR – 2015
Outline

• What?

• How?
  • Campaigns
  • Targets
  • Tool

• Evasion
Context: Operation Buthrap you say?
Operation Buhtrap – the basics

• Financially motivated group targeting banks and businesses in Russia

• Active since at least April 2014

• Uses spearphishing, exploit kits to run campaigns

• Uses different people to code malware, exploit, test

• Uses tools on sale in underground forums
Why are you talking about that?

• More and more, groups are targeting commercial entities

• They use techniques we used to see in espionage campaigns

• We have seen several big attacks on businesses in the past, we believe we will see more, and operation Buhtrap is a good case study
The beginnings

• We analyzed this, NSIS packed, first stage, which had interesting checks
The beginnings

• We analyzed this, NSIS packed, first stage, which had interesting checks
Stealthy

- Checks for system language, applications installed, URLs visited to decide which package to download
- Also checks for security software to modify which application version to install
Targets

• Looking at
  • Decoy documents
  • URLs and application installed
  • Domains used

• Businesses and more specifically accounting departments seemed to be the target of this group
Certificates

• As we will see later on, downloaded packages contained a lot of files

• Many of which were signed by valid certificates
Group

- While we progress in our research it became clear that this was a group of organized people
  - Malware coder
  - Exploit coder
  - Testers

- As will become apparent, they also had pretty good ties with cybercriminals selling tools and services in underground forums
This seemed like a suitable research

- Group of people launching spearphishing attacks against Russian businesses
- Using as much stealth as possible
- Code signing certificate usage
- Using modular code and 3rd party tools
Campaigns
Timeline

- **Start of the first campaign (first known activity)**: April 1, 2014
- **Start of the second campaign**: April 10, 2015
- **Passport Scan**: August 1, 2015
- **Return of the MWI**: October 1, 2015
- **Blog post released**: April 9, 2015
- **Flash Player bundle**: October 1, 2015
Tools – Overall Installation process

• Through spam, operators are ultimately trying to have full control of the victim computer.

1. User receives a spam
2. User opens infected Word attachment
3. Word document downloads additional module from external server
4. Cybercriminals can spy and control remotely the victim’s computer
Targets – Detection statistics

- Russia: 88%
- Ukraine: 10%
- Other: 2%
Targets

• Businesses, most probably accounting departments. Why this assumption?
• Decoy documents, applications and URLs check and finally domains
• Malicious domains used by cybercriminals:
  • store.kontur-expres.com ← "SKB Kontur has been simplifying business accounting in Russia since 1988"
  • help.b-kontur.org
  • forum.buhonline.info ← buhonline.ru: forum content directed towards accountant
  • topic.buhgalter-info.com
  • balans2w.balans2.com
Infection Vector

- Spearphishing with business oriented decoy documents
Infection Vector

- Spearphishing with business oriented decoy documents
Side Story - Microsoft Word Intruder?

- It is a kit, sold in underground forums that allow to build RTF documents exploiting several CVE
- Shows the connections of this group: they got it 1 year before public disclosure

A New Word Document Exploit Kit

April 01, 2015 | By Nart Villeneuve, Joshua Homan | Exploits, Threat Research

The tools used to create malicious documents that exploit vulnerabilities in Microsoft Word are now being advertised in underground forums and one new tool has emerged that provides the ability to track the effectiveness of campaigns. The builder, Microsoft Word Intruder (MWI), is advertised as an “APT” tool to be used in targeted attacks. It is accompanied by a statistics package known as “MWISTAT” that allows operators to track various campaigns.
Side Story - Microsoft Word Intruder

- Uses four exploits
  - CVE-2010-3333
  - CVE-2012-0158
  - CVE-2013-3906
  - CVE-2014-1761
- Two modes of operation: INTERNAL and EXTERNAL
- No decoy, malware payload must show one if needed
- Several modifications, we see the kit evolving through the buhtrap campaign as well
Tools – first stage

• The first stage implant makes tons of checks to make sure the system is valuable and not a researcher’s system
Tools – first stage

- The first stage implant makes tons of checks to make sure the system is valuable and not a researcher’s system.
Tools – first stage

• The first stage implant makes tons of checks to make sure the system is valuable and not a researcher’s system
Tools – Usage of Decoy Second Stage

• If those tests fail, it downloads a decoy package instead of the real second stage implant

• Remember this picture?
Tools – Usage of Decoy Second Stage

• In this case, the NSIS first stage implant downloads a fake 7z self-extracting executable
Tools – Usage of Decoy Second Stage

• If we look at the installation script in the downloaded second stage, we see that they are using a malicious way to install the decoy package

```plaintext
set S1=de
set S2=t.exe
call %S1%%%S2%
if %ERRORLEVEL% EQU 2 goto elv
if %ERRORLEVEL% EQU 0 goto end
call WLToolBar.msi /quiet
goto end
:elv
elevate.exe -c WLT.cmd
ping -n 20 localhost
```
Tools – Local Privilege Exploitation

- They have been using several different exploits

- First campaign was CVE-2013-3660 and Carberp trick in source code

- Then in subsequent campaigns, we saw CVE-2014-4113, CVE-2015-2546 and CVE-2015-2387 (part of the Hacking Team leak)

- Always had the x86 and x64 versions
Tools – Overall View of the Second stage Download

- When the checks are satisfied, downloads the second stage malicious payload used to spy on their targets
Tools – System Preparation

• xtm.exe - System preparation
Tools – mimikatz.exe

- Tool used by pentesters (and others!) to access an account

- Modified binary to issue following commands: `privilege::debug` and `sekurlsa::logonPasswords` to recover logon passwords
Tools – xtm.exe

• 1c_export: tries to add a user to system

• This package was no longer seen in later campaigns (NOT necessary for the initial compromise)
  • We have seen them later on they dropping it through the backdoor
Tools - Backdoor

• Impack.exe - Backdoor
Tools – Impack.exe

• Silent installation of litemanager, a remote administrator

• Supposedly legit but, why silent installer? Detected as a PUA (potentially unsafe application)
Tools – Main Buhratp module

• pn_pack.exe – Spying Module
Tools – pn_pack.exe

- Log all keystrokes and copy clipboard content
- Enumerate smart cards present on the system
- Handle C&C communications
Tools – pn_pack.exe

• Uses dll-sideloading and decrypt main module on the fly

• Uses well known application to hide
  • Yandex punto
  • The Guide
  • Teleport Pro
Tools – pn_pack.exe

- RC4 for communications, but also to encrypt strings. NW is XOR with preceding byte and then RC4 encrypted
- Two commands: download and execute module, download code and start new thread in it

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MZ</td>
<td>The data sent is an executable. The banker module will execute it through the CreateProcess API</td>
</tr>
<tr>
<td>LD</td>
<td>The data sent is code. The banker module will copy it into executable memory and will execute it by launching a new thread.</td>
</tr>
</tbody>
</table>

- only module present in later installment. Use existing functionalities to install all the remaining tools
New infection vector: Niteris EK
Timeline

Start of the first campaign (first known activity) 4/1/2014

Start of the second campaign 4/10/2015

Passport Scan 8/1/2015

Return of the MWI 10/1/2015

Blog post released 4/9/2015

Flash Player bundle 10/1/2015
Targets

- Still (Russian) businesses

- The dropper still contains the same script that checks for URLs, applications, debug app, etc
Infection Vector

- They are no longer using MWI for this campaign

- Spearphishing
  - Exploit Kit
  - Executable Attachments
Infection Vector – Executable attachments

- Passport scan
Infection Vector – Niteris EK

• Appeared in 2014

• Low prevalence, few malware distributed through it (ursnif, corkow)

• Flash exploit – CVE-2014-0569

Tools – Evolved First Stage Downloaders

• Distributed as Microsoft KB files
• One dropper was very different, not NSIS, heavy usage of RC4

• LOTS of detection for security products
  • Sandbox (Sandboxie, Norman)
  • Virtual Machines (VMWare, VirtualBox, QEMU)
  • Python/Perl
  • Wine
  • User interaction

• Downloads second stage if checks are satisfied
Tools – USB stealer

- One component that was signed with certificate was a USB stealer
- Copies file from drives A:\ and B:\ or USB drive to local folder
- Skips .pdf, .doc and .mp3
The return of the MWI kit
Timeline

- Start of the first campaign (first known activity)
  - 4/1/2014

- Blog post released
  - 4/9/2015

- Start of the second campaign
  - 4/10/2015

- Passport Scan
  - 8/1/2015

- Return of the MWI
  - 10/1/2015

- Flash Player bundle
  - 10/1/2015
Targets

• They shifted their focus
  • Businesses
  • Banks
Infection Vector – Microsoft Word Intruder via spam

• MWI again!
  • Possibly due to big rewrite
  • The overall infection workflow changed
Infection vector – Strategic Web Compromise

- Late October, we saw that Ammyy.com was distributing Buhtrap
Infection vector – Strategic Web Compromise

- Other malware were distributed through ammyy.com
  - Lurk downloader
  - Corebot
  - Ranbyus
  - Netwire RAT
Evasion
Evasion – bypassing AntiVirus

- Tries to prevent antivirus updates
- Tries to put their malware in exclusion list
- Different packages depending on which internet security product is installed
Evasion – Anti-Forensics

- mbrkiller.exe: NSIS installer that destroys MBR. Possibly used to wipe the computer after they are done with it

- damagewindow.exe: shows a pop up screen saying there was a HDD failure and user should reboot system
Thank you

Questions ?

@jiboutin