## Attack Patterns

stolen credentials were compiled in a list and used when the attackers needed to guess secret phrase in other locations.

### Trojan dropper (Spear phishing)

* previously known targeted attack campaign with Chinese origins.

### File Injection

* The "LHAFD.GCP" file is … essentially a backdoor, which is decoded by the loader module (svchost.exe). The decrypted file is injected into system memory and is responsible for communication with the C&C server.

## Campaigns

## Courses of Action (COA)

## Identity

קורבנות:

* Diplomatic
* Governmental
* scientific research organizations

## Indicators

### Victems Location

* region of Eastern Europe
* former USSR members
* countries in Central Asia

### Dropper

The embedded executable is a file-dropper, which extracts and runs three additional files.

* %TEMP%MSC.BAT
* %ProgramFiles%WINDOWS NTLHAFD.GCP (<- This file name varies)
* %ProgramFiles%WINDOWS NTSVCHOST.EXE

### MSC.BAT

* file has the following contents:
  + chcp 1251
  + :Repeat
  + attrib -a -s -h -r "%DROPPER\_FILE%"
  + del "%DROPPER\_FILE%"
  + if exist "%DROPPER\_FILE%" goto Repeat
  + del "%TEMP%msc.bat"
* first line of this file, which is a command to switch the codepage of an infected system to 1251.

### LHAFD.GCP

### General

* encrypted with RC4
* compressed with the "Zlib" library
* svchost.exe

### svchost.exe connection

* update.microsoft.com
* www.microsoft.com
* support.microsoft.com

## ​Intrusion Set

## Malware

### Trojan

### Backdoor

The "LHAFD.GCP" file is encrypted with RC4 and compressed with the "Zlib" library. This file is

essentially a backdoor, which is decoded by the loader module (svchost.exe). The decrypted file is injected into system memory and is responsible for communication with the C&C server.

## ​Observed Data

### File

File creation day:

* 19.05.2010
* 21.07.2010
* 04.09.2010
* 05.01.2011
* 14.03.2011
* 05.04.2011
* 23.06.2011
* 06.09.2011
* 21.09.2011
* 12.01.2012

Name of attachment filenames:

* Katyn\_-\_opinia\_Rosjan.xls
* FIEO contacts update.xls
* spisok sotrudnikov.xls
* List of shahids.xls
* Spravochnik.xls
* Telephone.xls
* BMAC Attache List - At 11 Oct\_v1[1].XLS
* MERCOSUR\_Imports.xls
* Cópia de guia de telefonos (2).xls
* Programme de fetes 2011.xls
* 12 05 2011 updated.xls
* telefonebi.xls

### URL

Hosts the malware tried to connect to in order to check Internet connection.

* update.microsoft.com
* www.microsoft.com
* support.microsoft.com

### Process

svchost.exe

## Report

## Threat Actors

מטרות:

* gather intelligence

המידע נאסף מ:

* computer systems
* personal mobile devices
* network equipment

המידע שנאסף:

## Tool

## Vulnerability\Exploit Targets

* CVE-2009-3129 (MS Excel)
* CVE-2010-3333 (MS Word)
* CVE-2012-0158 (MS Word)

{

"type": "attack-pattern",

"id": "attack-pattern--3098c57b-d623-4c11-92f4-5905da66658b",

"created": "2015-05-15T09:00:00.000Z",

"modified": "2015-05-15T09:00:00.000Z",

"object\_marking\_refs": [

"marking-definition--3444e29e-2aa6-46f7-a01c-1c174820fa67"

],

"name": "Initial Compromise",

"description": "As with most other APT groups, spear phishing is APT1’s most commonly used technique. The spear phishing emails contain either a malicious attachment or a hyperlink to a malicious file. The subject line and the text in the email body are usually relevant to the recipient. APT1 also creates webmail accounts using real peoples’ names — names that are familiar to the recipient, such as a colleague, a company executive, an IT department employee, or company counsel. The files they use contain malicious executables that install a custom APT1 backdoor that we call WEBC2-TABLE.",

"external\_references": [

{

"source\_name": "capec",

"description": "spear phishing",

"external\_id": "CAPEC-163"

}

],

"kill\_chain\_phases": [

{

"kill\_chain\_name": "mandiant-attack-lifecycle-model",

"phase\_name": "initial-compromise"

}

]

},

"type": "attack-pattern",

"id": "attack-pattern--1e2c4237-d469-4144-9c0b-9e5c0c513c49",

"created": "2015-05-15T09:00:00.000Z",

"modified": "2015-05-15T09:00:00.000Z",

"object\_marking\_refs": [

"marking-definition--3444e29e-2aa6-46f7-a01c-1c174820fa67"

],

"name": "Establishing a Foothold",

"description": "APT1 establishes a foothold once email recipients open a malicious file and a backdoor is subsequently installed. In almost every case, APT backdoors initiate outbound connections to the intruder’s 'command and control' (C2) server. While APT1 intruders occasionally use publicly available backdoors such as Poison Ivy and Gh0st RAT, the vast majority of the time they use what appear to be their own custom backdoors. APT1’s backdoors are in two categories: 'Beachhead Backdoors' and 'Standard Backdoors.' Beachhead Backdoors offer the attacker a toe-hold to perform simple tasks like retrieve files, gather basic system information and trigger the execution of other more significant capabilities such as a standard backdoor. APT1’s beachhead backdoors are usually what we call WEBC2 backdoors. WEBC2 backdoors are probably the most well-known kind of APT1 backdoor, and are the reason why some security companies refer to APT1 as the Comment Crew. A WEBC2 backdoor is designed to retrieve a webpage from a C2 server. It expects the webpage to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. WEBC2 backdoors are often packaged with spear phishing emails. Once installed, APT1 intruders have the option to tell victim systems to download and execute additional malicious software of their choice. The standard, non-WEBC2 APT1 backdoor typically communicates using the HTTP protocol (to blend in with legitimate web traffic) or a custom protocol that the malware authors designed themselves. The BISCUIT backdoor (so named for the command “bdkzt”) is an illustrative example of the range of commands that APT1 has built into its “standard” backdoors. APT1 has used and steadily modified BISCUIT since as early as 2007 and continues to use it presently. Some APT backdoors attempt to mimic legitimate Internet traffic other than the HTTP protocol. When network defenders see the communications between these backdoors and their C2 servers, they might easily dismiss them as legitimate network traffic. Additionally, many of APT1’s backdoors use SSL encryption so that communications are hidden in an encrypted SSL tunnel.",

"kill\_chain\_phases": [

{

"kill\_chain\_name": "mandiant-attack-lifecycle-model",

"phase\_name": "establish-foothold"

}

]

}

"type": "attack-pattern",

"id": "attack-pattern--19da6e1c-69a8-4c2f-886d-d620d09d3b5a",

"created": "2015-05-15T09:00:00.000Z",

"modified": "2015-05-15T09:00:00.000Z",

"object\_marking\_refs": [

"marking-definition--71f8e024-2c02-4350-a627-a71fa9de3437"

],

"external\_references": [

{

"source\_name": "capec",

"description": "spear phishing",

"external\_id": "CAPEC-163"

}

],

"name": "Spear Phishing Attack Pattern used by admin@338",

"description": "The preferred attack vector used by admin@338 is spear-phishing emails. Using content that is relevant to the target, these emails are designed to entice the target to open an attachment that contains the malicious PIVY server code.",

"kill\_chain\_phases": [

{

"kill\_chain\_name": "mandiant-attack-lifecycle-model",

"phase\_name": "initial-compromise"

}

]

},

{

"type": "indicator",

"id": "indicator--329ae6e9-25bd-49e8-89d1-aae4ca52e4a7",

"created": "2015-05-15T09:00:00.000Z",

"modified": "2015-05-15T09:00:00.000Z",

"object\_marking\_refs": [

"marking-definition--71f8e024-2c02-4350-a627-a71fa9de3437"

],

"name": "www.webserver.dynssl.com",

"description": "www.webserver.dynssl.com resolved to 113.10.246.30, 219.90.112.203, 219.90.112.203, 75.126.95.138, 219.90.112.197, and 202.65.222.45, which overlap with the gwx@123 IP addresses.",

"pattern": "[domain-name:value = 'www.webserver.dynssl.com' OR ipv4-addr:value = '113.10.246.30' OR ipv4-addr:value = '219.90.112.203' OR ipv4-addr:value = '75.126.95.138' OR ipv4-addr:value = '219.90.112.197' OR ipv4-addr:value = '202.65.222.45']",

"labels": [

"malicious-activity",

"attribution"

],

"valid\_from": "2015-05-15T09:00:00.000Z"

},

{