Dyre Banking Trojan

BY
Hailong Liu
Sixiao Long
Xiaoyu Zhang

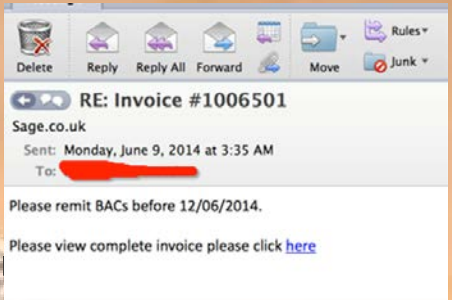
Introduction

- Also known as
  --Dyreza, Dyzap, and Dyranges
- Discovered
  --In early June 2014, by the Dell SecureWorks Counter Threat Unit(TM) (CTU) research team
- Banking Trojan
  -- Used to take money and login credentials from the victims' bank accounts
- RAT
  --Remote Access Trojan
- Target
  -- Account holders of Bank of America, Citibank, NatWest, RBS and Ulsterbank
- Dyre attack steals more than 1 million

Distribution

- Through spam **emails**
  --which contain Upatre downloader
- Executable in a **ZIP** attachment or as a malicious **URL**.
- User interaction is required to compromise the targeted system.
- Use different lures

- Injecting code into the victim's browser



RE: Invoice #1006501

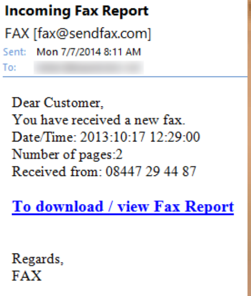
Sage.co.uk

Sent: Monday, June 9, 2014 at 3:35 AM

To: [redacted]

Please remit BACs before 12/06/2014.

Please view complete invoice please click here



Incoming Fax Report

FAX [fax@sendfax.com]

Sent: Mon 7/7/2014 8:11 AM

To: [redacted]

Dear Customer,
You have received a new fax.
Date/Time: 2013:10:17 12:29:00
Number of pages:2
Received from: 08447 29 44 87

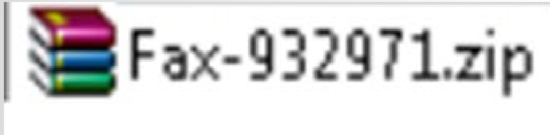
To download / view Fax Report

Regards,
FAX

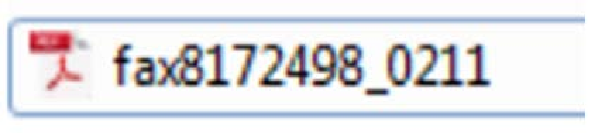
How it works

STEP 1: THE SPEAR PHISHING

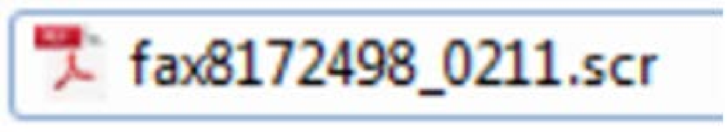
A victim receives an email that explains the attached invoice is for their review.



Fax-932971.zip



fax8172498_0211



fax8172498_0211.scr

←upatre downloader (executable)

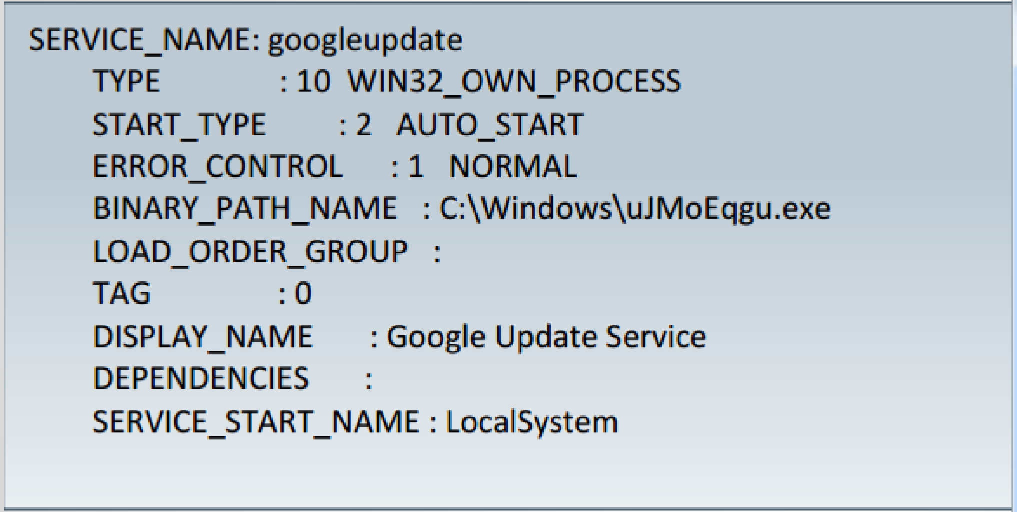
STEP 2: THE FIRST STAGE MALWARE IS EXECUTED

Upatre’s sole purpose is to download Dyre

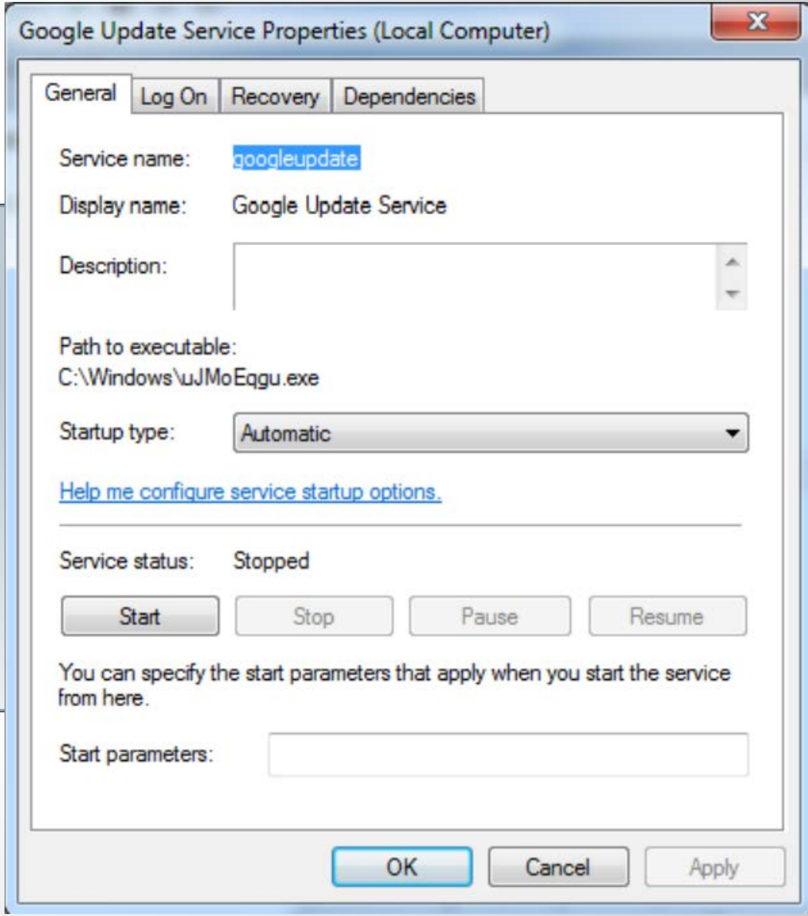
STEP 3: THE SECOND STAGE MALWARE IS EXECUTED

Once Dyre is loaded, Upatre removes itself

DYRE STAGE 1: ESTABLISHING PERSISTANCE



```
SERVICE_NAME: googleupdate
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Windows\uJMoEqgu.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Google Update Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```



Google Update Service Properties (Local Computer)

Service name: googleupdate

Display name: Google Update Service

Description:

Path to executable:
C:\Windows\uJMoEqgu.exe

Startup type: Automatic

Help me configure service startup options.

Service status: Stopped

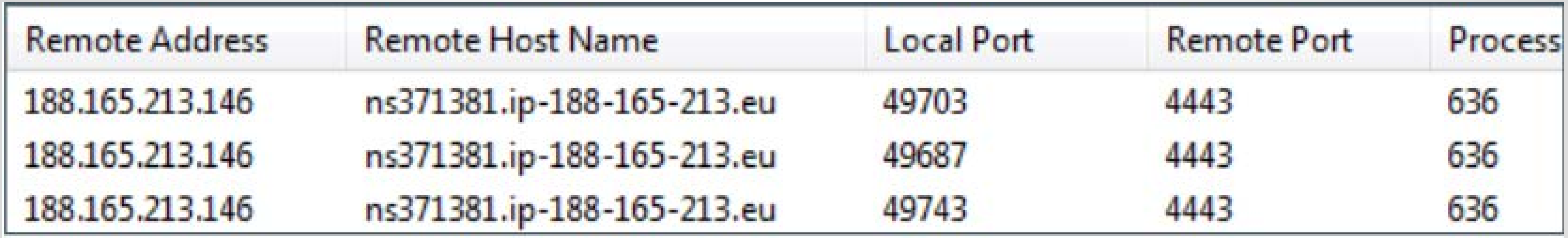
You can specify the start parameters that apply when you start the service from here.

Start parameters:

creating a service named “Google Update Service”,

injects malicious code into SVCHOST.EXE process

DYRE STAGE 2: ESTABLISHING A DARKNET



Remote Address	Remote Host Name	Local Port	Remote Port	Process
188.165.213.146	ns371381.ip-188-165-213.eu	49703	4443	636
188.165.213.146	ns371381.ip-188-165-213.eu	49687	4443	636
188.165.213.146	ns371381.ip-188-165-213.eu	49743	4443	636

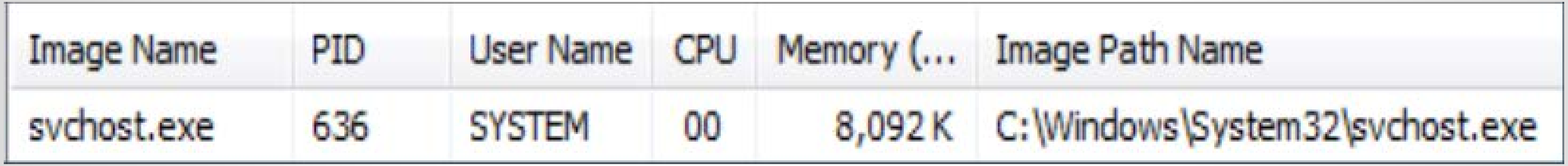


Image Name	PID	User Name	CPU	Memory (…	Image Path Name
svchost.exe	636	SYSTEM	00	8,092 K	C:\Windows\System32\svchost.exe

it hooks to the victim’s common browsers (Internet Explorer, Chrome & Firefox) in order to intercept credentials the user may enter when visiting any of the targeted bank sites.

DYRE STAGE 4 – EMAIL SPREADING

If Dyre detects that the OUTLOOK email client is installed, it will attempt to send email messages to various recipients with the DYRE payload attached as a zip file.

STEP 5: THE WIRE TRANSFER

The attacker logs into the account and transfers money to various offshore accounts.
There have been several reports of compromise resulting in losses of $500,000 to over $1,000,000 USD.

STEP 6: THE DDOS attack
  prevent victims from logging back into bank site.

How to Defense?

1.Strong security software.

2.Security-conscious Internet service provider (ISP).

3.Updating Windows on time .

4.Keeping your browser updating.

5.Be careful about the website you are going to.

Conclusion

- One of the most prominent banking trojans
- More powerful and robust.
- Advanced capabilities

  -- web fakes

  -- dynamic web injects

  -- a modular design

  -- multiple methods for maintaining command and control.
- Determination of threat actors targeting the financial vertical.

Reference

http://www.secureworks.com/cyber-threat-intelligence/threats/dyre-banking-trojan/

http://www.securityweek.com/dyre-banking-trojan-uses-worm-spread-microsoft-outlook

https://www.esentire.com/new-dyre-banking-threat-detected-dropbox-phishing-attacks/

http://www.enigmasoftware.com/dyredyrezatrojan-removal/
http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=%0a%09%09%09%09TrojanDownloader%3aWin32%2fUpatre.A%0a%09%09%09%09&wa=wsignin1.0
https://www.ltnow.com/dyre-banking-malware-email/
https://portal.sec.ibm.com/mss/html/en_US/support_resources/pdf/Dyre_Wolf_MSS_Threat_Report.pdf