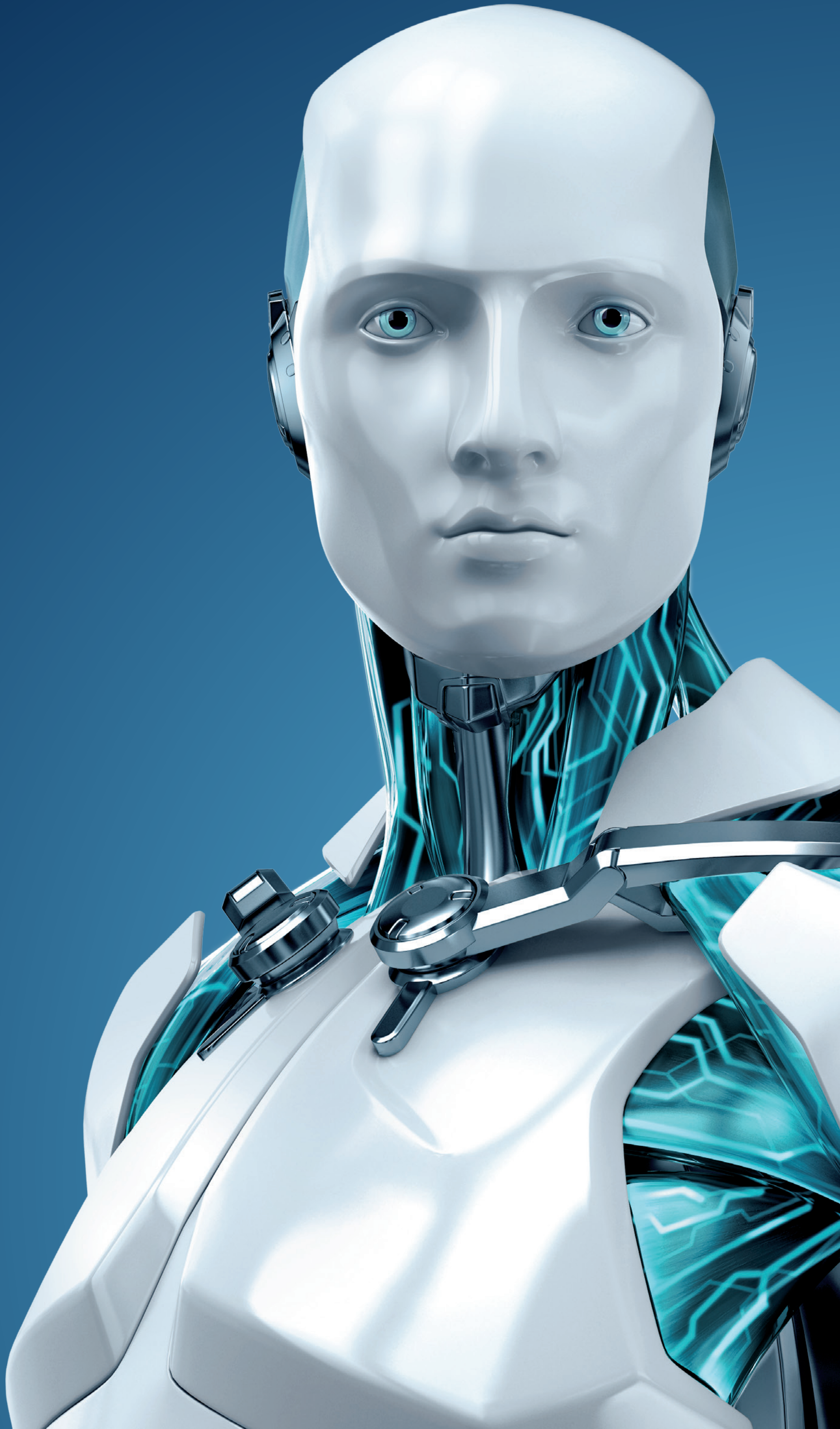
TECH BRIEF

Waski downloader spreads banker Trojan targeting users worldwide



ENJOY SAFER TECHNOLOGY®

WASKI DOWNLOADER SPREADS BANKER TROJAN TARGETING USERS WORLDWIDE

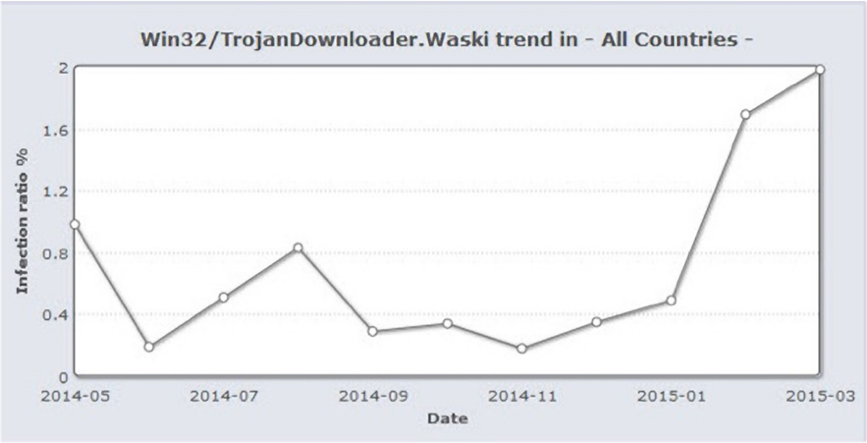
By Raphael Labaca Castro, ESET staff

Attention, financial institutions: There's been an uptick in activity by a powerful banking Trojan designed to steal your customers' login credentials. You can take a proactive approach by letting your clients know what to look for—and asking them to alert you immediately to any suspicious activity.

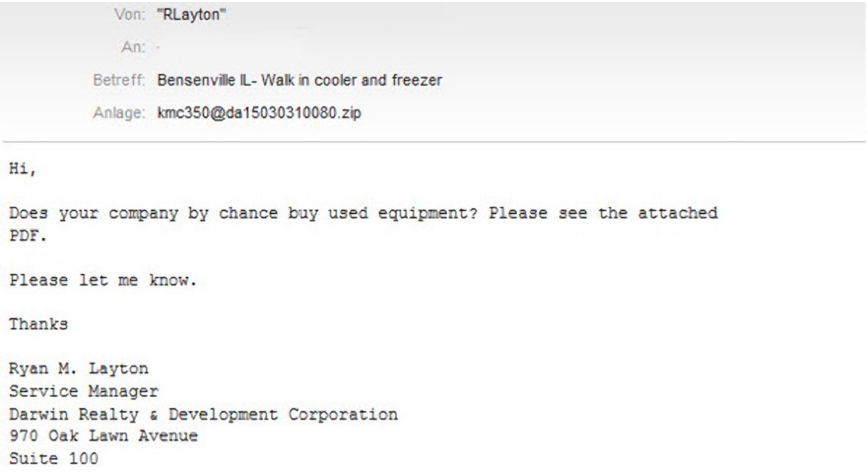
Here's how it works: If customers receive an unexpected email with a ZIP file attached, it could be a threat attempting to steal their banking login credentials. Known as Waski, it's detected by ESET as *Win32/TrojanDownloader.Waski*.

Waski is a so-called Trojan downloader, a small program that downloads additional malware that then is launched on the computer. Since the beginning of 2015, we have seen a significant increase in these detections. This is no coincidence as more and more criminals are using Waski to spread their malware on the Internet.

After detection spikes in Switzerland and Germany in March 2015, we've seen English-speaking regions affected in Australia, New Zealand, Ireland, United Kingdom, Canada, and the United States, among others.



It all starts with a seemingly harmless email. A potential victim receives the threat packaged in a ZIP file as an attachment to a spam



Von: "RLayton"

An: ·

Betreff: Bensenville IL- Walk in cooler and freezer

Anlage: kmc350@da15030310080.zip

```
Hi,

Does your company by chance buy used equipment? Please see the attached
PDF.

Please let me know.

Thanks

Ryan M. Layton
Service Manager
Darwin Realty & Development Corporation
970 Oak Lawn Avenue
Suite 100
```

email. The subject of the email is written in English, as well as the content, which often consists only of a single short sentence:

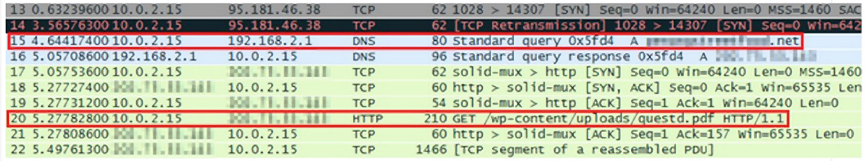
The figure above shows a typical email as spread by Waski. In this case, the email was allegedly sent by a company. The attachment contains a ZIP file containing Waski as an executable file. When started, it downloads other malicious software from a predefined web address.

Waski downloads online banking trojan

Waski is widely used by criminals to spread their malware and thus downloads a variety of malware. The particular one we investigated here downloads the banking Trojan Battdil, which is detected by ESET as *Win32/Battdil* or *Win64/Battdil*.

Waski comes in the form of an executable file with the icon of a PDF file. Once it's started, the malware first checks the victim's public IP address by requesting it from checkip.dyndns. Using the IP and other information of the victim's computer (computer name, Windows version, and service pack number), a unique identification number is calculated and then sent to the Waski command-and-control server (C&C).

Then Waski downloads an encrypted file (usually from a compromised website) that has a PDF file extension. But it is not a true PDF file; instead, it is a merge of two files: the malware *Win32/Battdil* and a regular PDF file. After that, Waski again contacts its C&C server and reports the successful compromise.



```
13 0.63239600 10.0.2.15      95.181.46.38   TCP    62 1028 > 14307 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SAC
14 3.56576300 10.0.2.15      95.181.46.38   TCP    62 [TCP Retransmission] 1028 > 14307 [SYN] Seq=0 Win=642
15 4.64417400 10.0.2.15      192.168.2.1    DNS    80 Standard query 0x5fd4  A [redacted].net
16 5.05708600 192.168.2.1    10.0.2.15      DNS    96 Standard query response 0x5fd4  A [redacted]
17 5.05753600 10.0.2.15      [redacted]     TCP    62 solid-mux > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
18 5.27727400 [redacted]     10.0.2.15      TCP    60 http > solid-mux [SYN, ACK] Seq=0 Ack=1 Win=65535 Len
19 5.27731200 10.0.2.15      [redacted]     TCP    54 solid-mux > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
20 5.27782800 10.0.2.15      [redacted]     HTTP  210 GET /wp-content/uploads/questd.pdf HTTP/1.1
21 5.27808600 [redacted]     10.0.2.15      TCP    60 http > solid-mux [ACK] Seq=1 Ack=157 Win=65535 Len=0
22 5.49761300 [redacted]     10.0.2.15      TCP  1466 [TCP segment of a reassembled PDU]
```

What does Battdil do?

Win32/Battdil consists of two parts: an injector and a payload. The injector consists of an EXE file, and the payload contains a DLL file that is stored in the original file. Often, the task of the injector is to inject the payload using DLL injection into a Windows process, as we see here with *Win32/Battdil*.

The payload of *Win32/Battdil* has the ability to intercept the login credentials for online banking in many of major browsers like Internet Explorer, Firefox, Chrome, etc. In addition, the websites of banks can be manipulated so that the victim does not get to see the original website, but a modified version.

This means that when they visit the website, some additional information is required such as the PIN Number from the credit card, which is then sent to the attacker. The collected information is sent encrypted via SSL to the C&C server. *Win32/Battdil* also has the ability to connect to its C&C server anonymously using the Invisible Internet Project (I2P).

Conclusion

Waski, first discovered at the end of 2013, has become increasingly popular because criminals can use it to spread their threats in Europe and North America. Protect your financial institution and your customers by alerting users that they should avoid opening emails with attachments from unknown sources. Second, remind them to keep security software installed and updated on their computers and devices. ESET offers a range of solutions for home and business which can protect from phishing attacks, banking Trojans and other cyber threats.

Hashes

Win32/Waski

1b893ca3b782679b1e5d1afecb75be7bcc145b5da21a30f6c18dbbc9c6de4e7 (SHA-256).

Win32/Battdil

Injector: 9b313e9c79921b22b488a11344b280d4cec9dd09c2201f9e5aaf08a115650b25 (SHA-256)

Payload: f8eccfebda8a1e0caabbe23a8b94d7ced980353a9b3673a4173e24958a3bdbb9 (SHA-256)

- *Research collaboration from Dominik Reichel*