Barracuda Threat Spotlight: New URL File Outbreak Could be a Ransomware Attempt

By Barracuda Networks

Published: 2018-04-10 · Archived: 2026-04-06 00:34:19 UTC

We're closely tracking an alarming threat that's currently aiming to take advantage of careless or untrained users in a possible effort to distribute ransomware and other forms of malware—here's what we've found.

Highlighted Threat: Attackers are using a variety of techniques in an attempt to launch a Quant Loader trojan capable of distributing ransomware and password stealers.

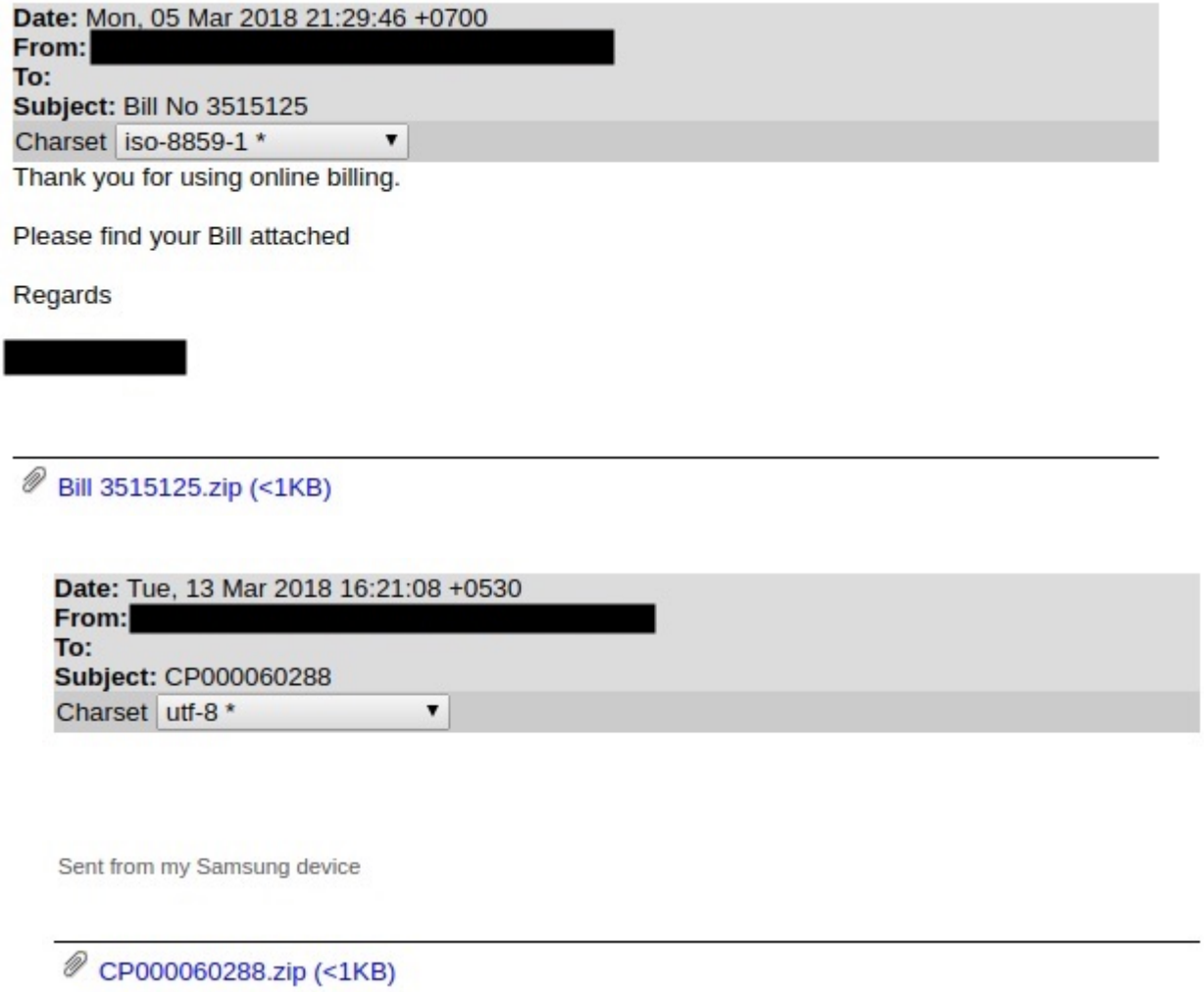
The Details:

In the world of email, an unfamiliar file extension—especially one that is compressed alone in a ZIP file—is often a sure sign of a new malware outbreak. This was no exception when zipped Microsoft internet shortcut files with a ".url" file extension started showing up in emails claiming to be billing documents last month. These shortcut files use a variation on the CVE-2016-3353 proof-of-concept, containing links to JavaScript files (and more recently Windows Script Files). However, in this instance the URL was prefixed with "file://" rather than "http://" which fetches them over Samba rather than through a web browser. This has the benefit of executing the contained code using WScript under the current user's profile rather than requiring browser exploitation, although it does prompt the user before doing so. The remote script files are heavily obfuscated, but all result in downloading and running Quant Loader when allowed to execute.

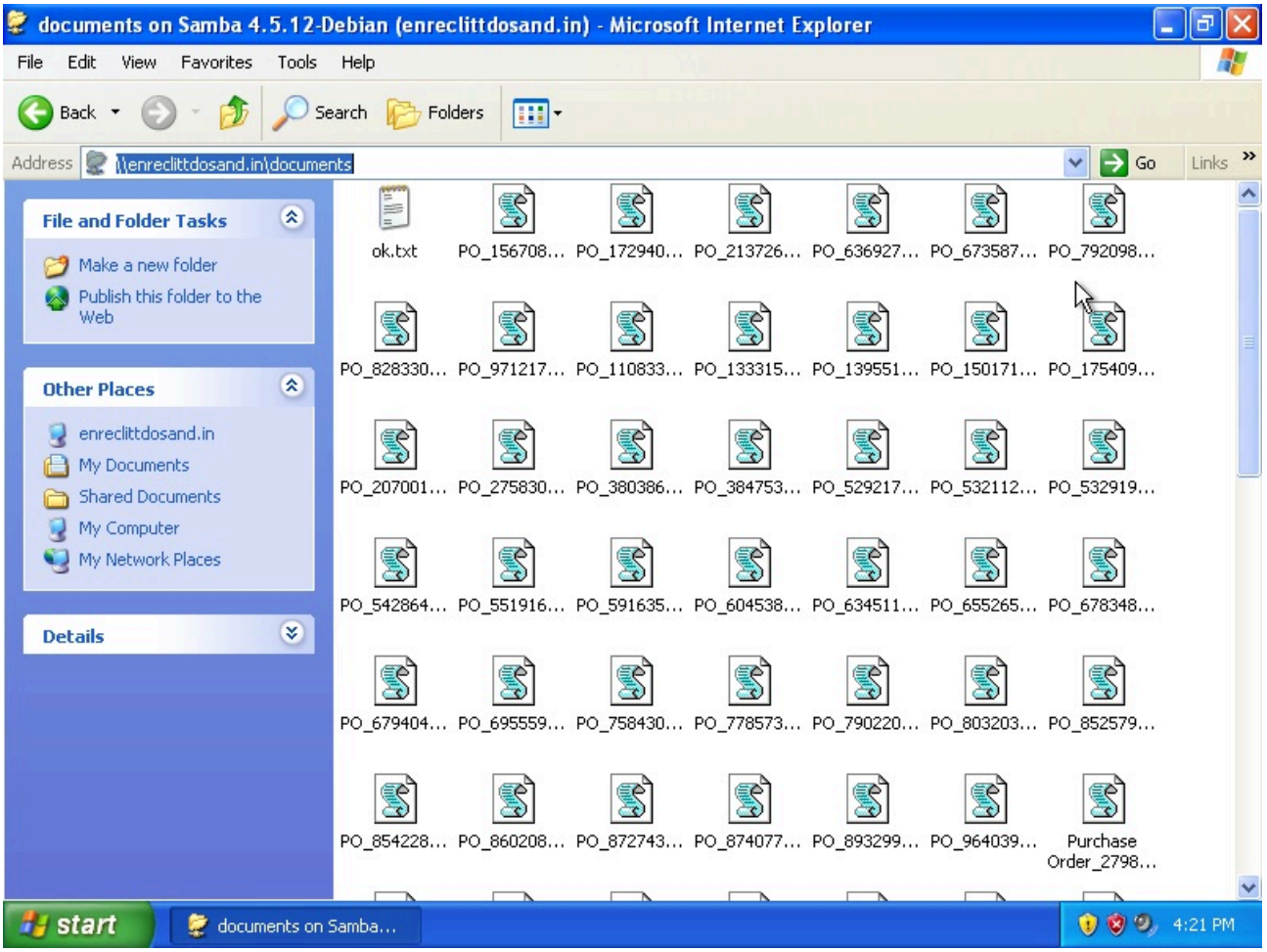
Based on past attacks, Quant Loader is a trojan that typically distributes malware such as ransomware and password stealers. It is sold on underground forums and allows the user to configure the payload(s) upon infection

using a management panel. Configurable malware offered for sale such as this is becoming more widespread, which allows malware development to be separated from distribution.

The campaign itself has been composed of a number of mini-campaigns—each lasting for a less than a day. They are utilizing an email content and file name pattern (with some emails having no text content and only a subject line), a single domain serving malicious script files over Samba, and a single variant of Quant being distributed from a handful of domains.



The Samba shares are publicly accessible while still active as shown in the image below. Interestingly, attempting to access the URLs via HTTP has led to redirects at times, resulting in a random key generator file to be downloaded. Fortunately, these are generally flagged as malicious by most antivirus software. Based on the research we've done tracking this campaign—it isn't showing up daily, but has shown up numerous times in March and April.



While attackers attempt to devise novel approaches for tricking users into infecting themselves, these can often lend themselves to being more easily spotted by those with security knowledge. Avoiding file types in emails that you are unfamiliar with is a good starting point, and certainly don't allow scripts to run that originated from files in email as well. Many techniques rely on social engineering and untrained or careless users rather than highly sophisticated attacks and exploits. Not only are exploits easier to detect than techniques that rely on user interaction, but they require significant resources to discover and utilize, aside from being regularly patched by software vendors—which is a major obstacle for cybercriminals.

To recap, the techniques used in these attacks are:

Phishing – emails sent to persuade the recipient into acting on their requests

Social Engineering – attackers engage with recipients in order to gain their trust and act on their malicious request

Exploit – CVE-2016-3353 was used to circumvent the browser and execute malicious scripts in user-space

Obfuscation – malicious scripts are heavily obfuscated to prevent or slow static analysis efforts

Take Action:

User Security Training and Awareness — Employees should be regularly trained and tested to increase their security awareness of various targeted attacks. Simulated attack training is by far the most effective form of training. A solution like Barracuda PhishLine provides comprehensive, SCORM-compliant user training and testing as well as phishing simulation for emails, voicemail, and SMS along with other helpful tools to train users to identify cyberattacks.

Additionally, layering employee training with an email security solution that offers sandboxing and advanced threat protection should block malware before it ever reaches the corporate mail server. And, for protection against messages that contain malicious links, you can deploy anti-phishing protection that includes Link Protection to look for links to websites that contain malicious code. Links to these compromised websites are blocked, even if those links are buried within the contents of a document.

Real-Time Spear Phishing and Cyber Fraud Defense — Barracuda Sentinel is a cloud service that utilizes AI to learn an organization's communications history and prevent future spear phishing attacks. It combines three powerful layers: an artificial intelligence engine that stops spear phishing attacks in real time and identifies the most high-risk individuals inside the company; domain fraud visibility using DMARC authentication to guard against domain spoofing and brand hijacking; and fraud simulation training for high-risk individuals.

Jonathan Tanner

Jonathan is a Senior Security Researcher at Barracuda Networks. Connect with him on LinkedIn here.

Source: https://blog.barracuda.com/2018/04/10/barracuda-threat-spotlight-new-url-file-outbreak-could-be-a-ransomware-attempt/