TA505 Group Adopts New ServHelper Backdoor and FlawedGrace RAT

bleepingcomputer.com/news/security/ta505-group-adopts-new-servhelper-backdoor-and-flawedgrace-rat/

Ionut Ilascu

By
Ionut Ilascu

- January 10, 2019
- 04:26 AM
- 0

Malware researchers discovered two new malware families distributed through phishing campaigns last year carried out by the TA505 cybercriminal group: ServHelper backdoor with two variants and FlawedGrace remote access trojan (RAT).

The threat actor continues to target organizations in the financial and retail sectors, the researchers say, using Microsoft Word, Microsoft Publisher, and PDF files pull the malware on the victim computer host.

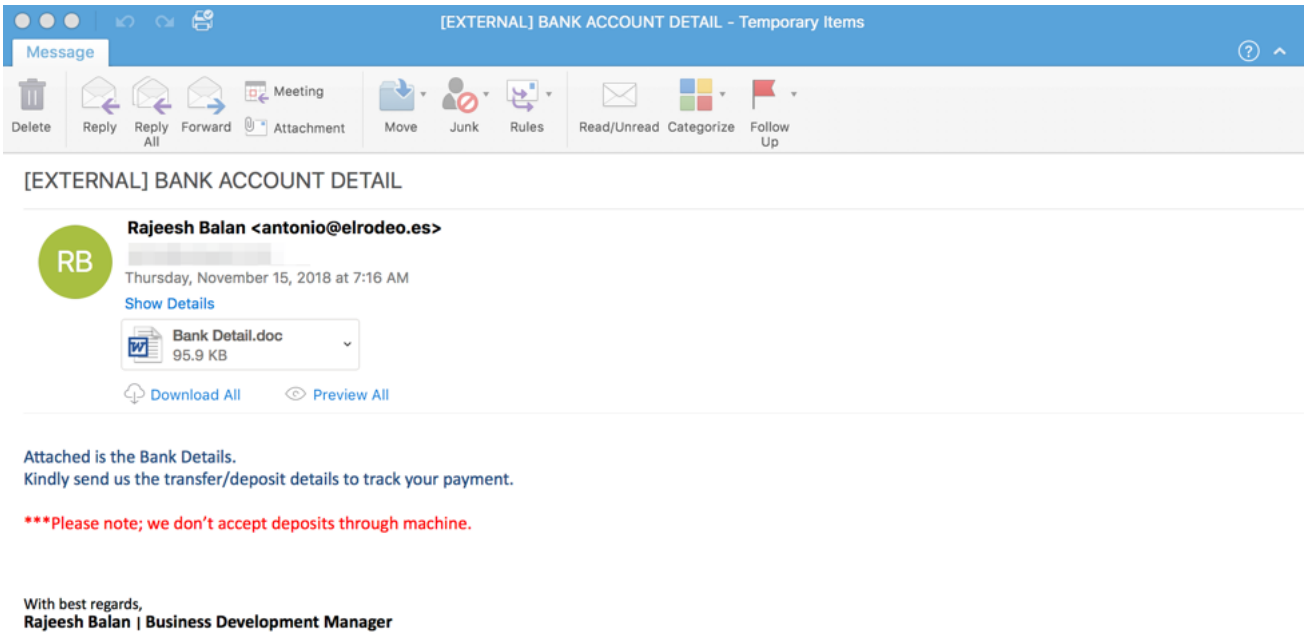
TA505, the name given by Proofpoint, has been in the cybercrime business for at least four years. This is the group behind the infamous Dridex banking trojan and Locky ransomware, delivered through malicious email campaigns via Necurs botnet.

Other malware associated with TA505 include Philadelphia and GlobeImposter ransomware families.

ServHelper delivered in three campaigns

A first salvo of malicious messages was shot on November 9, 2018. It was a small campaign with several thousand emails delivering Word and Publisher documents laced with hostile macros.

A larger campaign with tens of thousands of emails occurred six days later and carried messages with .DOC, .PUB, and .WIZ documents, all specific to the same Microsoft Office components mentioned above.



In a third session, observed on December 13, the threat actor mixed in PDF files with URLs purporting to lead to an Adobe update. Following the link took the potential victim to a fake "Adobe PDF Plugin" webpage that led to ServHelper.

Proofpoint, who spotted these campaigns and analyzed the two malware families, says that the distribution is not focused on a particular region on the world, and the focus is on financial services organizations.

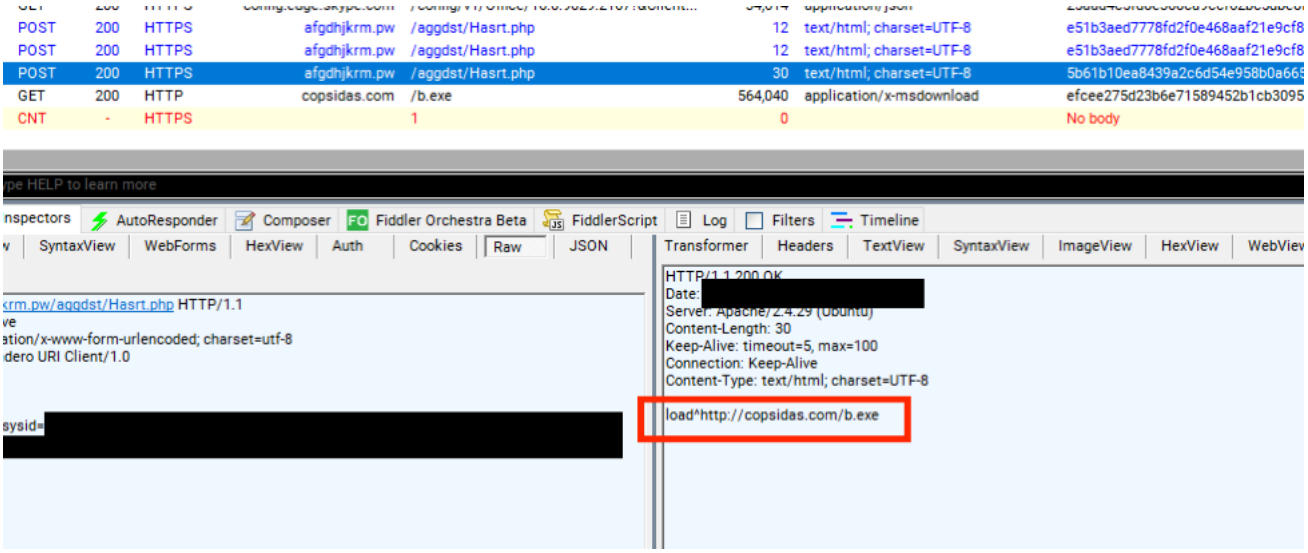
The infrastructure used for running these campaigns remains unknown for the time being, but it does not present the hallmarks specific to Necurs botnet.

Actively developed, ServHelper comes in two flavors

The purpose of the macro was to download and execute a variant of ServHelper that set up reverse SSH tunnels that enabled access to the infected host through the Remote Desktop Protocol (RDP) port 3389.

"Once ServHelper establishes remote desktop access, the malware contains functionality for the threat actor to “hijack” legitimate user accounts or their web browser profiles and use them as they see fit," researchers from Proofpoint explain in an analysis released today.

The other ServHelper variant does not include the tunneling and hijacking capabilities and functions only as a downloader for the FlawedGrace RAT.

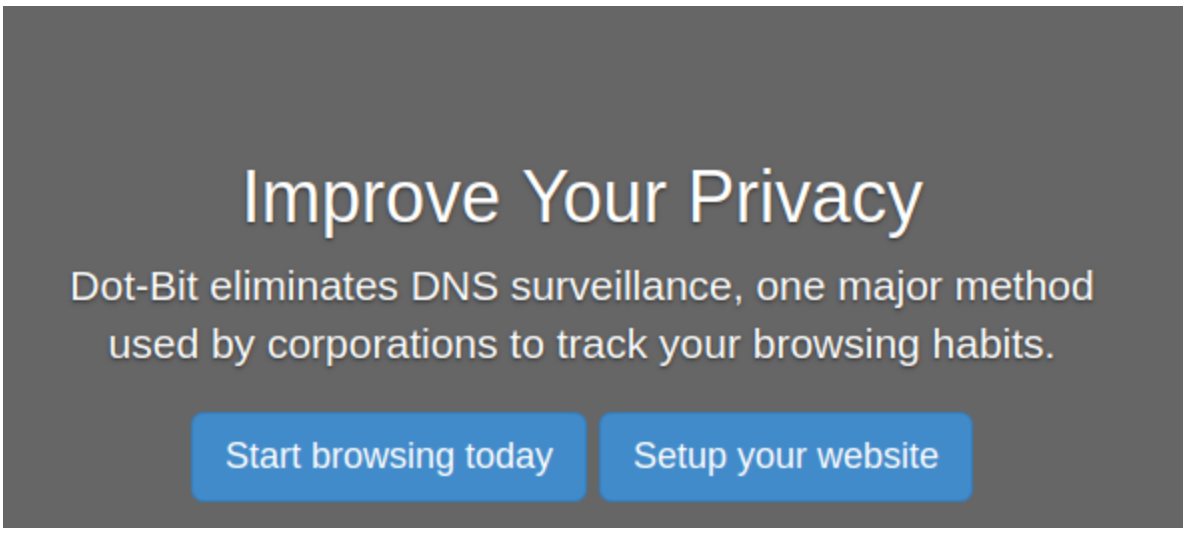


ServHelper is written in Delphi and its developers continue to update it with new features and commands. Proofpoint says that almost every new campaign reveals a changed variant of the malware.

Use of decentralized DNS

To protect the command and control (C2) servers against takedown efforts, the developer(s) uses the .bit Top-Level Domain (TLD) for the Domain Name System (DNS) servers.

Researchers found two such DNS servers resolving the IP addresses for four ServHelper's C2 servers: dedsolutions[.]bit and arepos[.]bit.

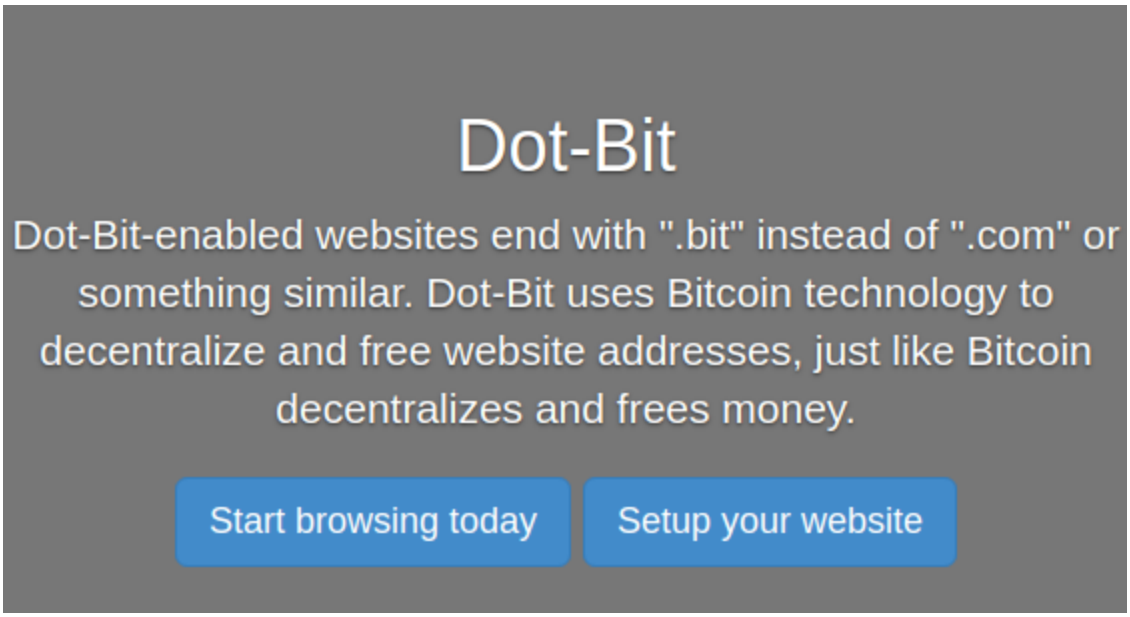


Internet TLDs like .com and .org and Country Code TLDs (ccTLD) designated for a particular country are maintained by the Internet Corporation for Assigned Names and Numbers (ICANN).

Security researchers and law enforcement agencies can ask ICANN to force a domain registry or registrar to shut-down, seize or sinkhole a domain name.

A .bit TLD does not fall under the umbrella of ICANN and is instead available through Namecoin cryptocurrency's blockchain transaction database.

The domain name is shared over a peer-to-peer network, making it fully decentralized and immune to any government or organization's efforts to regulate, suspend, or sinkhole it. Other decentralized TLDs are .emc, .lib, .bazar, .coin.



Proofpoint told BleepingComputer that not all C2 infrastructure uses .bit domains and can be taken down. "In other cases, particularly those using crypto dns, defenders need to rely on layered security to block related traffic," they added.

FlawedGrace is a tough nut to crack

Proofpoint is not at the first encounter with the FlawedGrace RAT, as the malware caught the researchers' eye since early November 2017.

Although multiple variants exist, some as early as August 2017, it was not seen actively distributed until recently.

"Per the malware’s debug strings, significant development took place during the end of 2017. The ServHelper campaigns were distributing version 2.0.10 of the malware [built on November 20, 2017]," the researchers note in their report.

They also point out that FlawedGrace is a full-featured RAT written in C++ and that it is a very large program that "extensive use of object-oriented and multithreaded programming techniques." As a consequence, getting familiar with its internal structure takes a lot of time and is far from a simple task.

After analyzing both malware families, the researchers were able to conclude that there are sufficient discrepancies in the coding style and techniques to be the work of different developers.

Update [01.10.2019]: The article erroneously mentioned that Necurs botnet was used to run the email campaigns that delivered ServHelper and FlawedGrace malware. We have updated it to reflect that and that the TA505 group is behind the new malware families. We also included comments from Proofpoint.

Related Articles:

BPFDoor malware uses Solaris vulnerability to get root privileges

BPFDoor: Stealthy Linux malware bypasses firewalls for remote access

Hackers target Russian govt with fake Windows updates pushing RATs

Fake Windows exploits target infosec community with Cobalt Strike

Malicious PyPI package opens backdoors on Windows, Linux, and Macs

- Backdoor
- Botnet
- RAT
- SSH
- TA505

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

You may also like: