New Evidence Proves Ongoing WIZARD/LUNAR SPIDER Collaboration

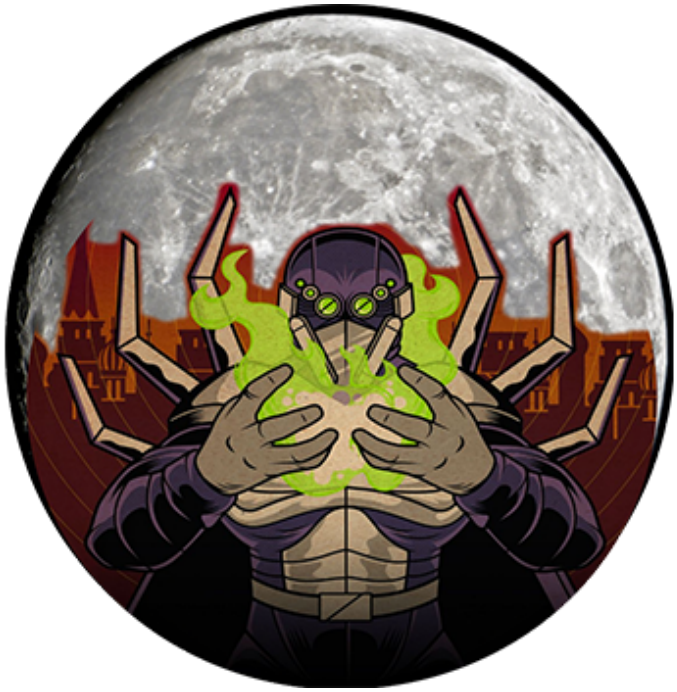
crowdstrike.com/blog/wizard-spider-lunar-spider-shared-proxy-module/

March 20, 2019

New Evidence Proves Ongoing WIZARD SPIDER / LUNAR SPIDER Collaboration

March 20, 2019

Brendon Feeley and Brett Stone-Gross Research & Threat Intel



On March 17, 2019, CrowdStrike® Intelligence observed the use of a new BokBot (developed and operated by LUNAR SPIDER) proxy module in conjunction with TrickBot (developed and operated by WIZARD SPIDER), which may provide WIZARD SPIDER with additional tools to steal sensitive information and conduct fraudulent wire transfers. This activity also provides further evidence to support the existence of a flourishing relationship between these two actors.

WIZARD SPIDER's TrickBot banking malware began distributing a new proxy module named `shadDll` to group tags (gtags) prefixed with `sin` and `tin`. These gtags have previously been associated with LUNAR SPIDER's BokBot (a.k.a. IcedID) malware, which was discussed in a previous blog.

The module contains identical functionality to that of the BokBot proxy module. The new proxy module incorporates many of the most potent BokBot features within the extensible, modular framework of the TrickBot malware. Binary code analysis revealed that the `shadDll` **TrickBot module is 81 percent similar to the BokBot proxy module with 99 percent confidence**.

Man-in-the-Middle Attacks

This new TrickBot module, `shadDll ,` is primarily responsible for performing man-in-the-middle (MITM) attacks against web browsers on infected hosts, achieved by hooking networking functions and installing illegitimate SSL certificates. Once the malware is able to intercept SSL traffic, it can use the various BokBot configuration entries to strategically redirect web traffic, inject code, take screenshots, and otherwise manipulate victims' browsing experience.

The `shadDll` module contains typical characteristics of a TrickBot module. More explicitly, the modules are dynamic link libraries (DLLs), they contain no TrickBot encrypted strings, and they have the standard TrickBot exports of `Start, Control` and `Release` . Although the `shadDll` module contains no TrickBot-encrypted strings, it does contain strings obfuscated using the custom XOR encoding used in the BokBot proxy module.

Hard-Coded DN Values

Of particular interest is the following hard-coded distinguished name (DN) values, which are identical to the ones found within the illegitimate certificates that the BokBot proxy module uses for performing MITM attacks.

```
C=US; O=VeriSign, Inc.; OU=VeriSign Trust Network; OU=(c) 2006 VeriSign, Inc. - For authorized use only; CN=VeriSign Class 3 Public Primary Certification Authority  - G5
```

Further Solidification of Two eCrime Groups

This development between WIZARD SPIDER and LUNAR SPIDER further solidifies the connection between the two groups, which stretches back to the *Dyre* (a.k.a. *Dyreza*) and *Neverquest* era. CrowdStrike Intelligence will continue to monitor this intriguing working relationship and mutual integration. A detailed analysis of the BokBot proxy module that is now being distributed by TrickBot is presented in this follow-up blog post.

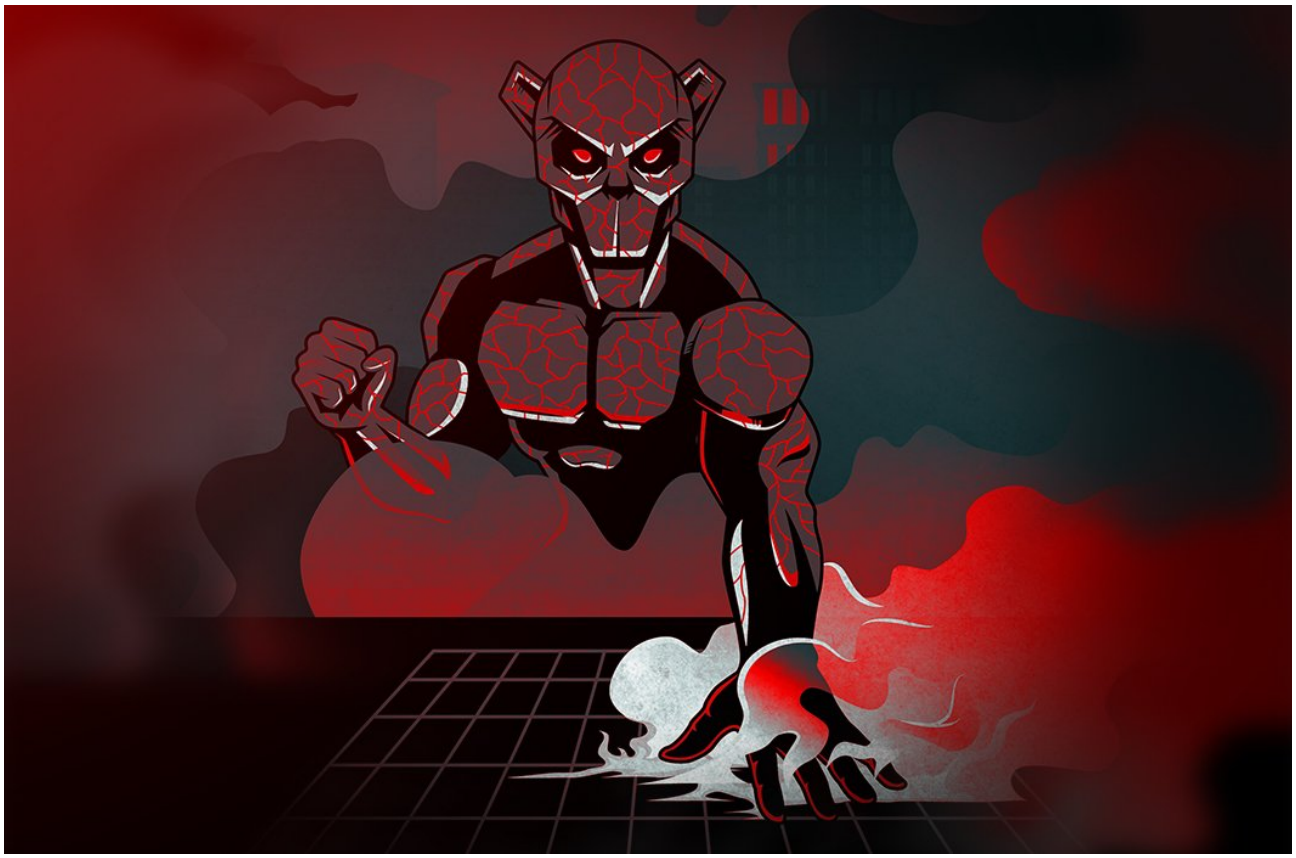
Indicators of Compromise (IOCs)	
Module Name	**SHA256 Hash**

shadDll32	dfea3d7607e72d4dff86be0ba30ec0620dc54d5d2a50799bbefe1e495e9accdd
shadDll64	2b5c064e269247be0dc1a4a20a7968206c9b82219daab7b10994f52770f68661

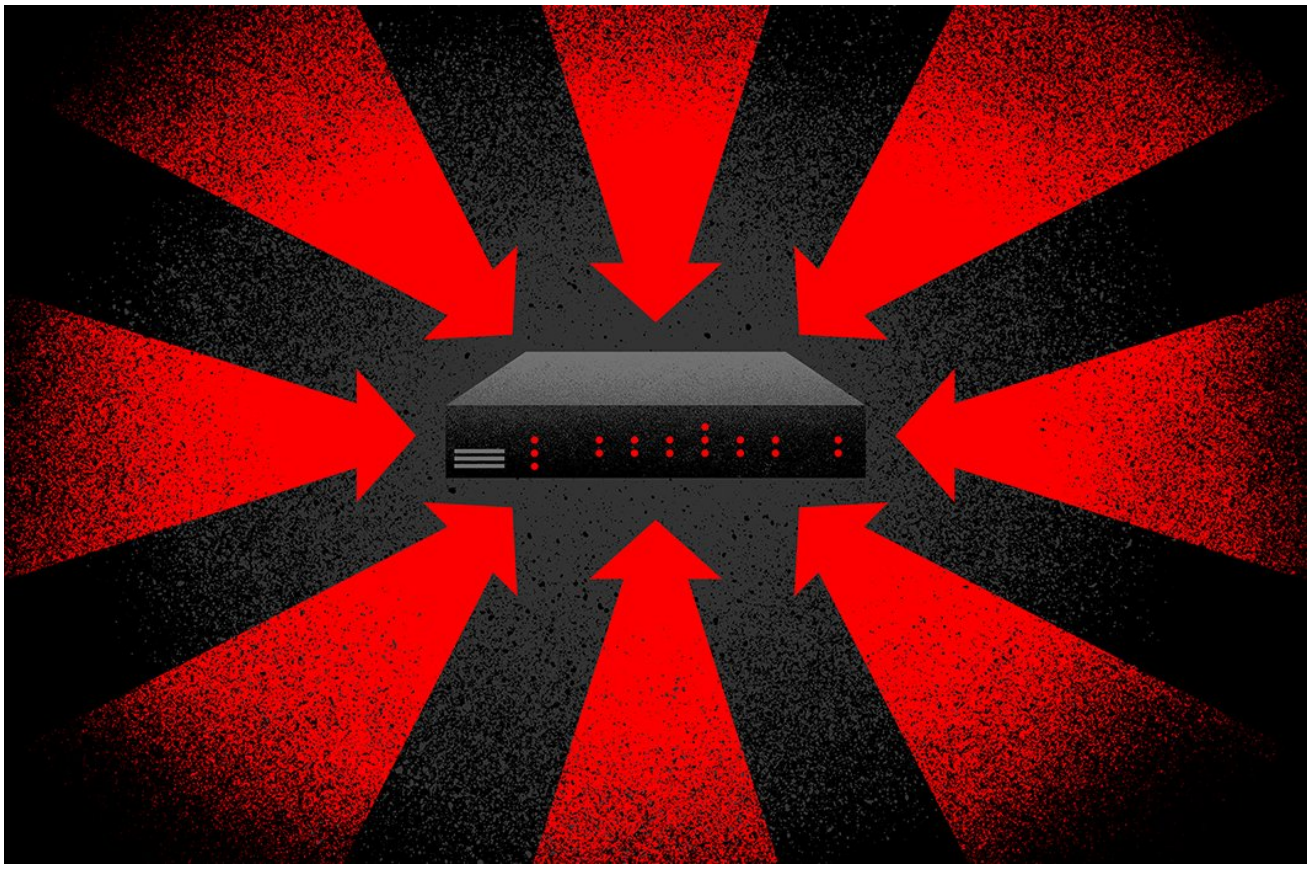
Additional Resources

- *Download the 2020Global Threat Report.*
- *Read our report on Falcon X Automated Threat Intelligence to learn why actionable threat intelligence is the next step in SOC evolution.*
- *Learn more about comprehensive endpoint protection with the CrowdStrike Falcon platform by visiting the product page.*
- *Test CrowdStrike next-gen AV for yourself. Start your free trial of Falcon Prevent™ today.*

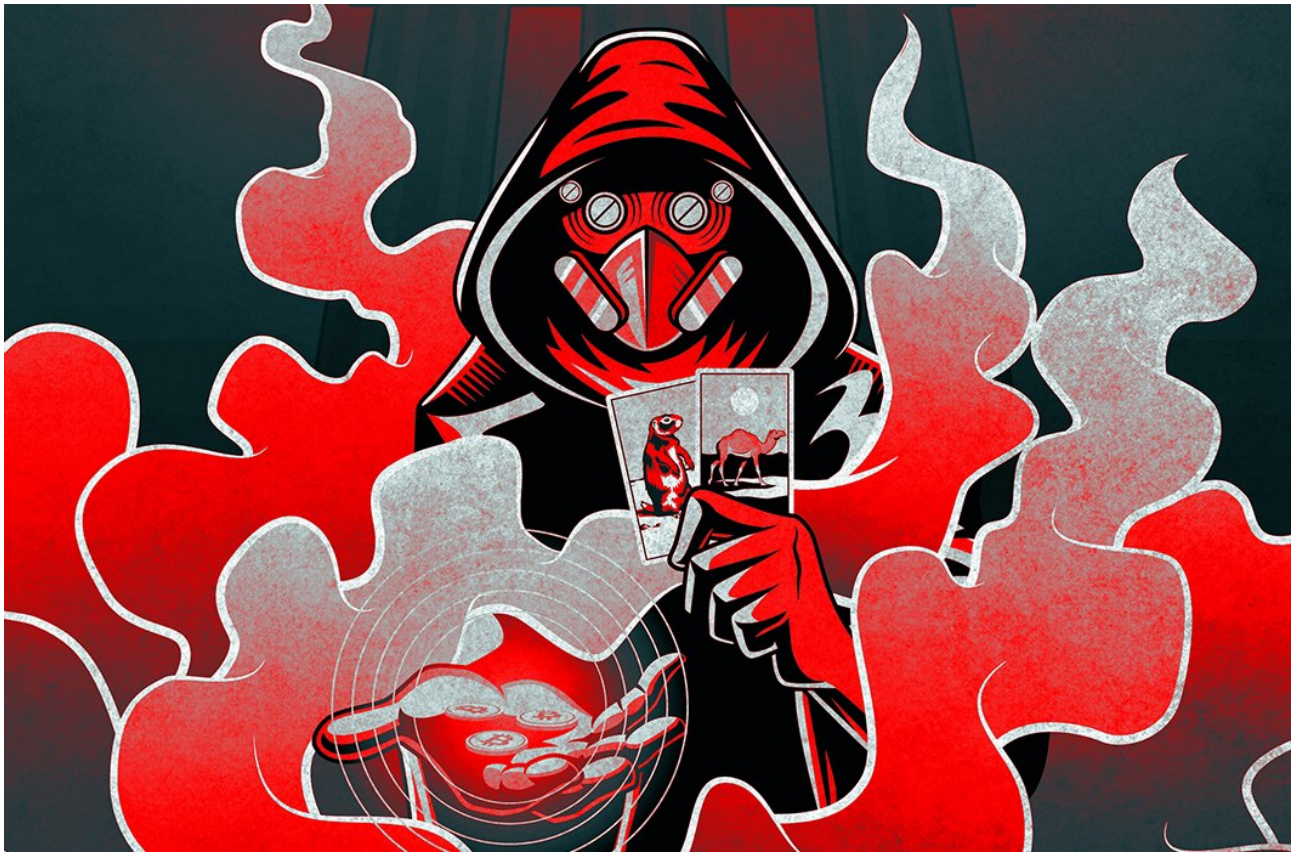
Related Content



Who is EMBER BEAR?



A Tale of Two Cookies: How to Pwn2Own the Cisco RV340 Router



PROPHET SPIDER Exploits Citrix ShareFile Remote Code Execution Vulnerability CVE-2021-22941 to Deliver Webshell