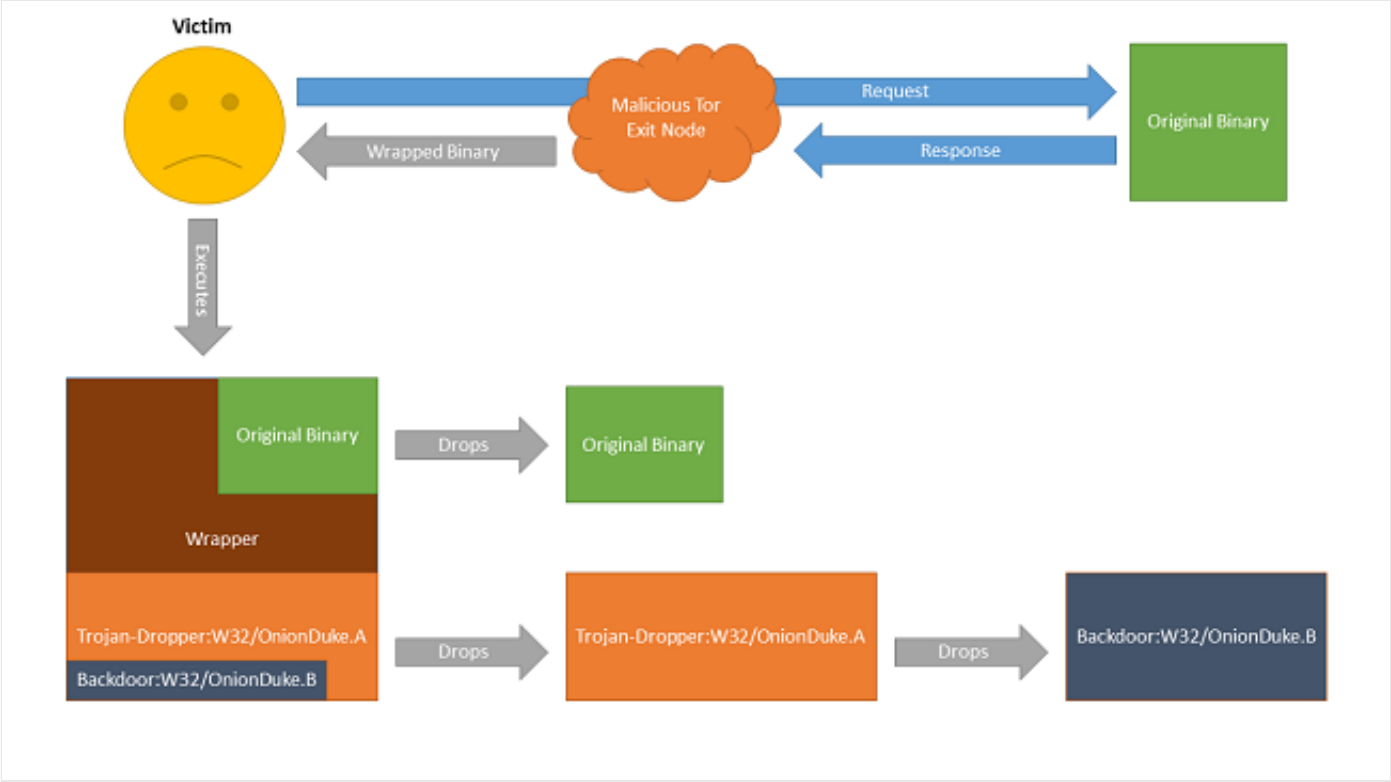
OnionDuke: APT Attacks Via the Tor Network - F-Secure Weblog : News from the Lab

Recently, research was published identifying a Tor exit node, located in Russia, that was consistently and maliciously modifying any uncompressed Windows executables downloaded through it. Naturally this piqued our interest, so we decided to peer down the rabbit hole. Suffice to say, the hole was a lot deeper than we expected! In fact, it went all the way back to the notorious Russian APT family MiniDuke, known to have been used in targeted attacks against NATO and European government agencies. The malware used in this case is, however, not a version of MiniDuke. It is instead a separate, distinct family of malware that we have since taken to calling OnionDuke. But lets start from the beginning.

When a user attempts to download an executable via the malicious Tor exit node, what they actually receive is an executable "wrapper" that embeds both the original executable and a second, malicious executable. By using a separate wrapper, the malicious actors are able to bypass any integrity checks the original binary might contain. Upon execution, the wrapper will proceed to write to disk and execute the original executable, thereby tricking the user into believing that everything went fine. However, the wrapper will also write to disk and execute the second executable. In all the cases we have observed, this malicious executable has been the same binary (SHA1: a75995f94854dea8799650a2f4a97980b71199d2, detected as **Trojan-Dropper:W32/OnionDuke.A**). This executable is a dropper containing a PE resource that pretends to be an embedded GIF image file. In reality, the resource is actually an encrypted dynamically linked library (DLL) file. The dropper will proceed to decrypt this DLL, write it to disk and execute it.



A flowchart of the infection process

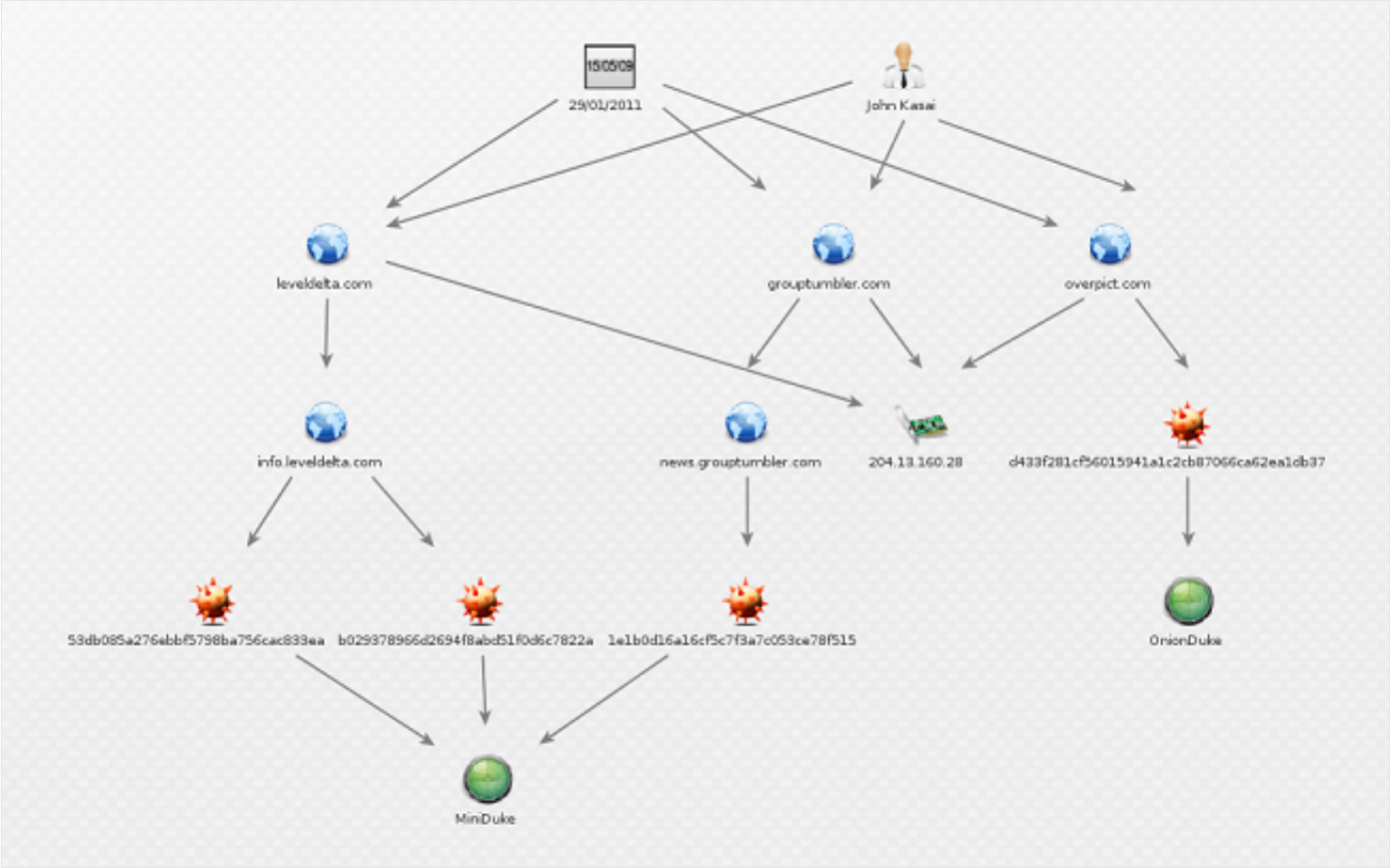
Once executed, the DLL file (SHA1: *b491c14d8cfb48636f6095b7b16555e9a575d57f*, detected as **Backdoor:W32/OnionDuke.B**) will decrypt an embedded configuration (shown below) and attempt to connect to hardcoded C&C URLs specified in the configuration data. From these C&Cs the malware may receive instructions to download and execute additional malicious components. It should be noted, that we believe all five domains contacted by the malware are innocent websites compromised by the malware operators, not dedicated malicious servers.

```
1  ---
2  cfg:
3    timestamp: 0
4    webhosts:
5      - url: http://                                menu.php
6        param: ghdfjk
7        key: 2905129839
8      - url: http://                                menu.php
9        param: fagac
10       key: 2905129839
11     - url: http://                                menu.php
12       param: hjkujl
13       key: 2905129839
14     - url: http://                                menu.php
15       param: qgjkcl
16       key: 2905129839
17     - url: http://                                menu.php
18       param: xjnioa
19       key: 2905129839
20   plugins:
21     check_new_sec: 3600
```

A screenshot of the embedded configuration data

Through our research, we have also been able to identify multiple other components of the OnionDuke malware family. We have, for instance, observed components dedicated to stealing login credentials from the victim machine and components dedicated to gathering further information on the compromised system like the presence of antivirus software or a firewall. Some of these components have been observed being downloaded and executed by the original backdoor process but for other components, we have yet to identify the infection vector. Most of these components don't embed their own C&C information but rather communicate with their controllers through the original backdoor process.

One component, however, is an interesting exception. This DLL file (SHA1 *d433f281cf56015941a1c2cb87066ca62ea1db37*, detected as **Backdoor:W32/OnionDuke.A**) contains among its configuration data a different hardcoded C&C domain, *overpict.com* and also evidence suggesting that this component may abuse Twitter as an additional C&C channel. What makes the *overpict.com* domain interesting, is it was originally registered in 2011 with the alias of "*John Kasai*". Within a two-week window, "*John Kasai*" also registered the following domains: *airtravelabroad.com, beijingnewsblog.net, grouptumbler.com, leveldelta.com, nasdaqblog.net, natureinhome.com, nestedmail.com, nostressjob.com, nytunion.com, oilnewsblog.com, sixsquare.net* and *ustradecomp.com*. This is significant because the domains *leveldelta.com* and *grouptumbler.com* have previously been identified as C&C domains used by MiniDuke. This strongly suggests that although OnionDuke and MiniDuke are two separate families of malware, the actors behind them are connected through the use of shared infrastructure.



A visualization of the infrastructure shared between OnionDuke and MiniDuke

Based on compilation timestamps and discovery dates of samples we have observed, we believe the OnionDuke operators have been infecting downloaded executables at least since the end of October 2013. We also have evidence suggesting that, at least since February of 2014, OnionDuke has not only been spread by modifying downloaded executables but also by infecting executables in .torrent files containing pirated software. However, it would seem that the OnionDuke family is much older, both based on older compilation timestamps and also on the fact that some of the embedded configuration data make reference to an apparent version number of 4 suggesting that at least three earlier versions of the family exist.

During our research, we have also uncovered strong evidence suggesting that OnionDuke has been used in targeted attacks against European government agencies, although we have so far been unable to identify the infection vector(s). Interestingly, this would suggest two very different targeting strategies. On one hand is the "*shooting a fly with a cannon*" mass-infection strategy through modified binaries and, on the other, the more surgical targeting traditionally associated with APT operations.

In any case, although much is still shrouded in mystery and speculation, one thing is certain. While using Tor may help you stay anonymous, it does at the same time paint a huge target on your back. It's never a good idea to download binaries via Tor (or anything else) without encryption. The problem with Tor is

that you have no idea who is maintaining the exit node you are using and what their motives are. VPNs (such as our Freedome VPN) will encrypt your connection all the way through the Tor network, so the maintainers of Tor exit nodes will not see your traffic and can't tamper with it.

Samples:

- a75995f94854dea8799650a2f4a97980b71199d2
- b491c14d8cfb48636f6095b7b16555e9a575d57f
- d433f281cf56015941a1c2cb87066ca62ea1db37

Detected as: **Trojan-Dropper:W32/OnionDuke.A**, **Backdoor:W32/OnionDuke.A**, and **Backdoor:W32/OnionDuke.B**.

Post by — Artturi (@lehtior2)