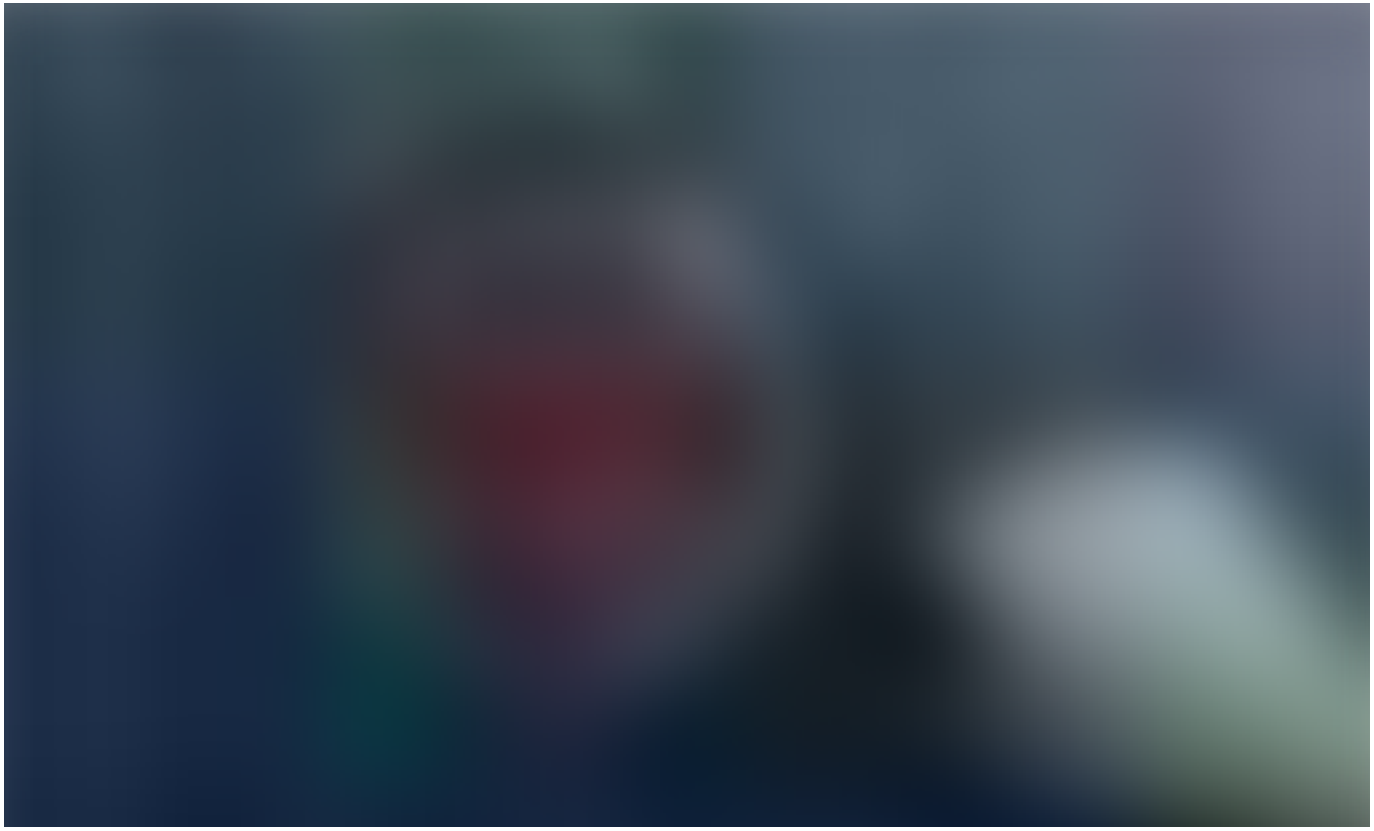
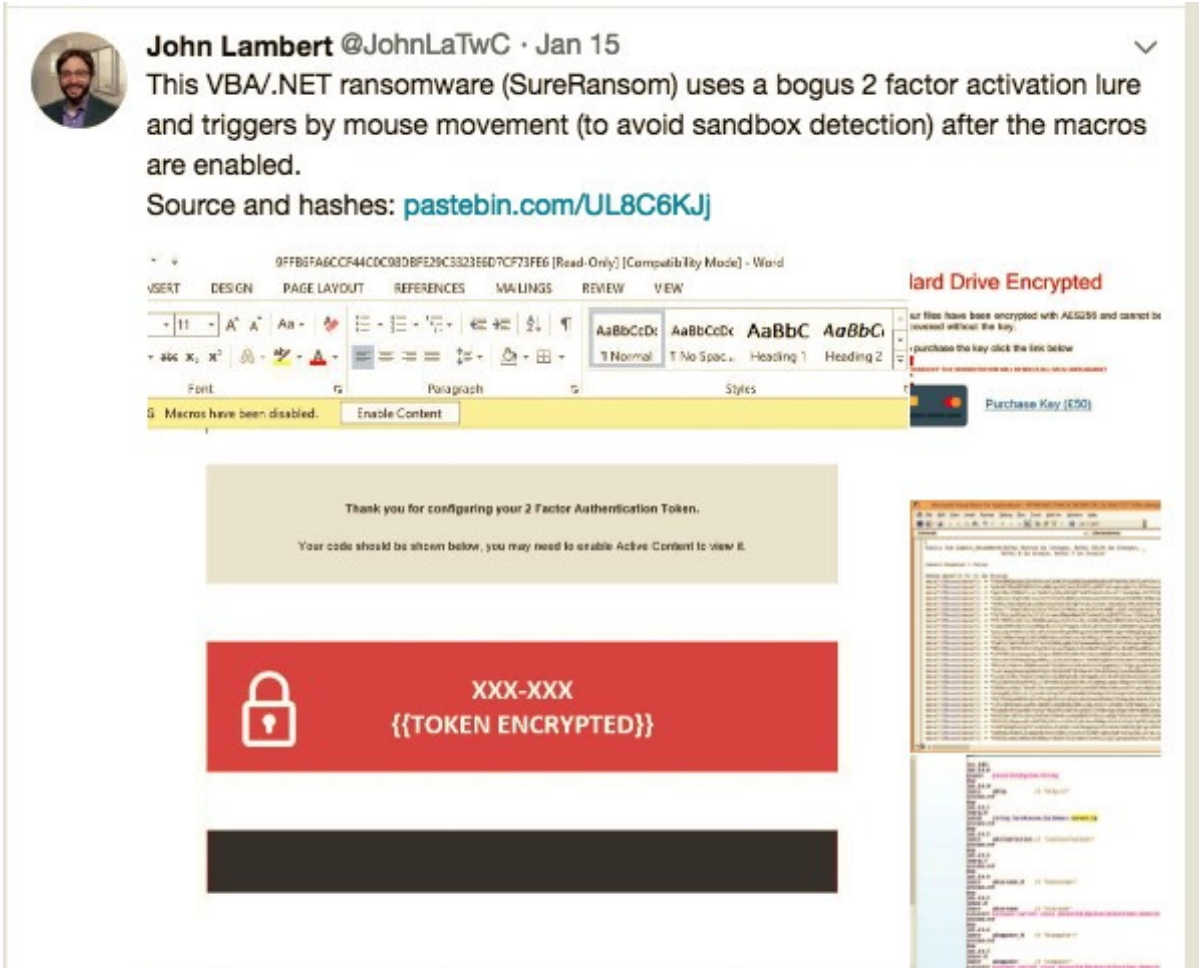
Detecting and Tracking the Red-Team

Netscylla Cyber Security Follow
Jan 22, 2018 · 4 min read



Last week we noticed this tweet on twitter from @JohnLaTwc:
https://twitter.com/JohnLaTwC/status/952948929628291072



We are big fans of John's tweets, and often use his discoveries to help build simulated malware campaigns for clients in Red-Teaming. This one was particularly interesting so we decided to dive into this one a little deeper.

The macro payload can be found here:

- https://pastebin.com/raw/UL8C6KJj

Payloads

There appears to be different payloads targeted at different Microsoft Operating Systems:

- Windows 7
- Windows 8- 8.1
- Windows 10

Netscylla decided to take a look at the Windows 10 payload (payloadv10.exe). It looks like it has already been uploaded to virus total and hybrid analysis from @CryptoInsane (twitter).

- https://www.virustotal.com/en/file/0acc9adbbdbd6db359552e2919aabc3ca4a42a28b3b7c3d26fb8f0699d23bdc2/analysis/
- https://www.reverse.it/sample/0acc9adbbdbd6db359552e2919aabc3ca4a42a28b3b7c3d26fb8f0699d23bdc2?environmentId=100

SureRansom.exe appears to be the real binary compiled name, and initial inspection looks like some form of British Ransomware demanding £50GBP to recover your files.

Further examination of the hybrid analysis and virus total reports, reveals the following IP addresses:

- 138.68.176.166

Whois on IP Address

The IP address belongs to cloud infrastructure provider Digital Ocean, this is likely the Command and Control interface for this piece of malware?

> *NetRange: 138.68.0.0–138.68.255.255*
>
> *CIDR: 138.68.0.0/16*
>
> *NetName: DIGITALOCEAN-15*

Reverse DNS: competitivebeauty.com

DomainTools.com data

Diving Deeper into the Payloadv10.exe

First we give the executable a once over with PEStudio for some hints to its maker, operation and possible code-base.

PEStudio: libraries informs us that it is a .Net application

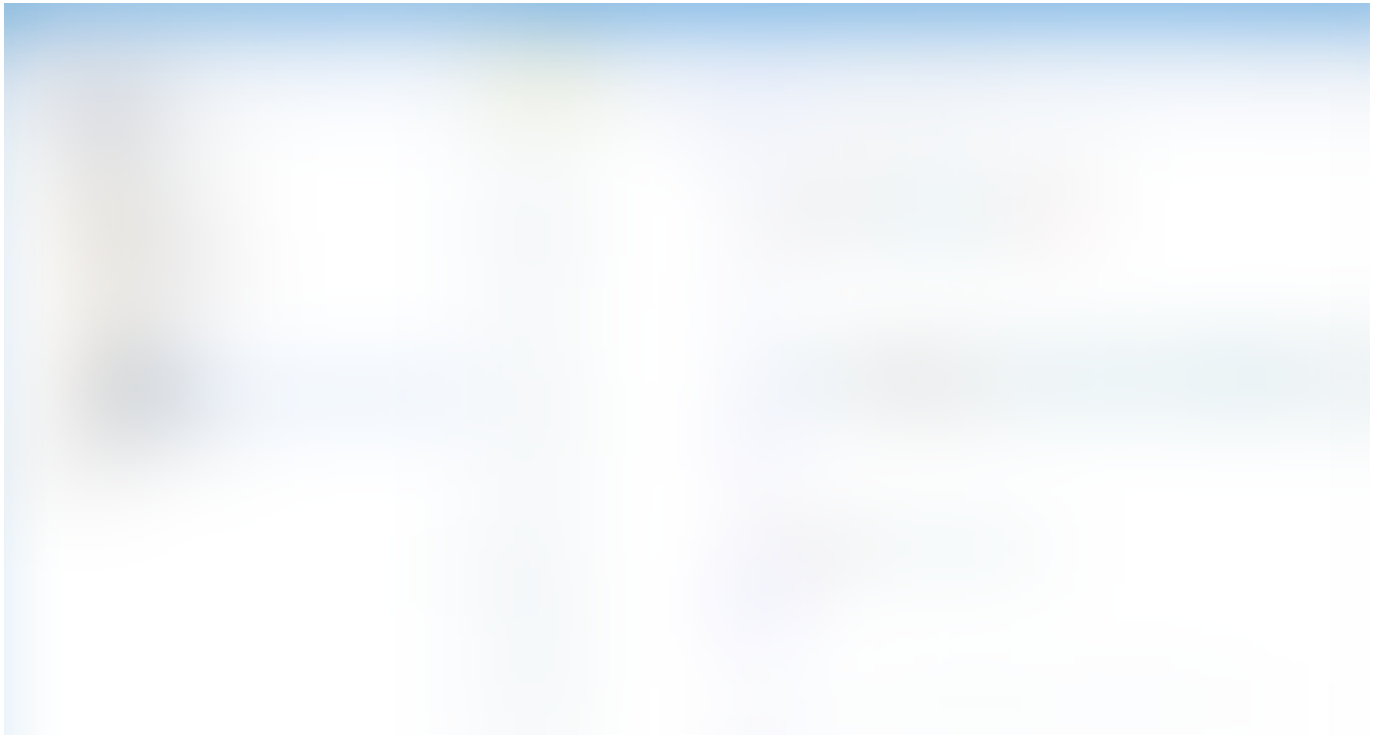
There is a big clue in the debug path:

PEStudio: Debug Path leaks author information

Now we have some hints that the author is Surecloud and that this executable is part of a Red-Team, penetration test or ransomware simulation!

Lets take this a little bit further....

The executable is a .Net compiled executable so we can use JustDecompile to disassemble the application into .Net classes and procedures.



The program's main class: identifying called classes and procedures.

This executable has the following operations:

- ping
- sendFiles
- sendUserDetails

CallHome IP matches the C2 addresses discovered earlier

The malware collects information on local and domain users

The malware sends all collected data unencrypted over the public internet.

Did we forget something? Isn't this meant to be ransomware…

Not really, as the decompiled code clearly indicates this is a simulation.

Yes, its only a simulation...

LinkedIn quick search for Surecloud, confirms a professional Penetration Test Team in United Kingdom:

Ransom? What Ransom?

Looking at the decompiled code, there is no functionality to process or take payments. This '*malware*' is only **a simulated exercise**!

Disclaimer

The information contained in this website is for general information purposes only. The information is provided by Netscylla and whilst we endeavour to keep it up-to-date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to the website or the information, products, services, or related graphics contained on the website for any purpose. Any reliance you place on such information is therefore strictly at your own risk.

In no event will we be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of this website.

Red Team | Blue Team | Phishing | Malware | Reversing

9 claps



WRITTEN BY

Netscylla Cyber Security

Follow

Interesting thoughts and opinions from the field of cyber security in general, focusing mainly on penetration testing and red-teaming.

Write the first response

More From Medium

Also tagged Red Team

Cyber Exercising, Red Teaming and Pentesting

Jon Lorains in The Startup
Jul 24 · 7 min read ★

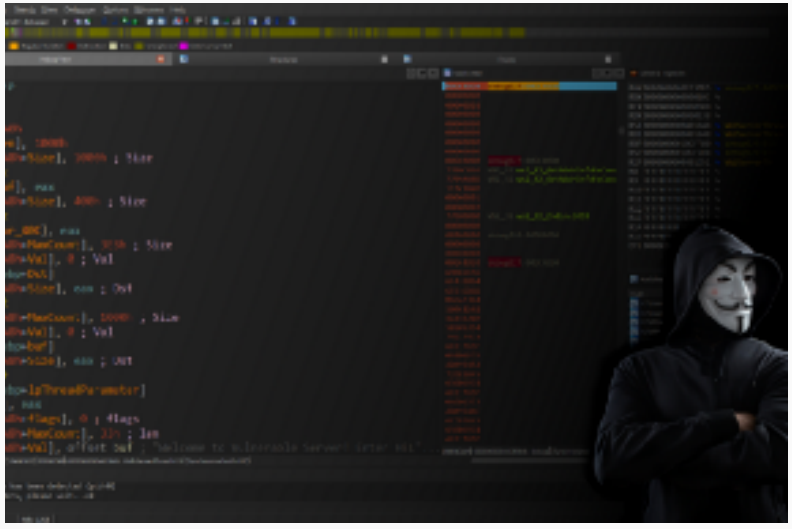
24

Also tagged Reversing

Windows-Based Exploitation — VulnServer TRUN Command Buffer Overflow

Andreas Poyiatzis in InfoSec Write...
May 30 · 6 min read ★

172



Also tagged Blue Team

Blue Team 101

Dylan Williams in The Lavender...
Jul 19 · 5 min read ★

5