Advanced Persistent Speaker ☺

BOTCONF 2022 – LIGHTNING TALK

C:> whoami /all

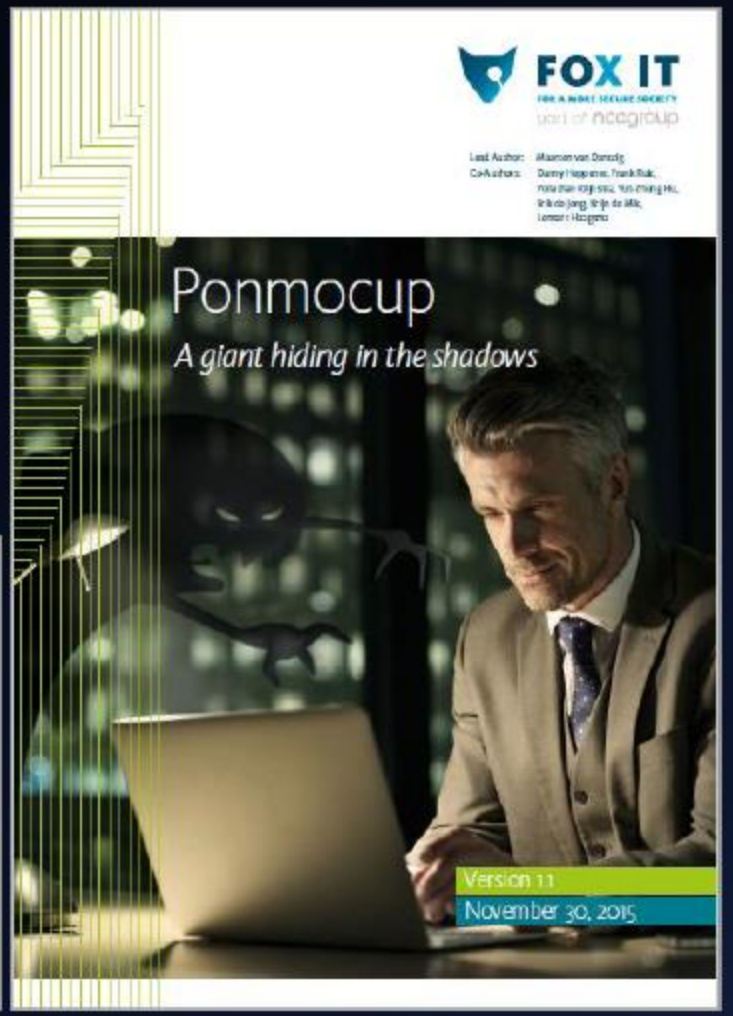
- Tom Ueltschi
- Swiss Post CERT / SOC / CSIRT since 2007 *(13 years!)*
- Focus & Interests: Malware Analysis, Threat Intel, Threat Hunting, Red / Purple Teaming
- Member of many trust groups & infosec communities
- FIRST SIG member (malware analysis, red teaming, CTI)
- Twitter: @c_APT_ure

BotConf speaker history

- 2013 - My Name is Hunter, Ponmocup Hunter
- 2014 - Ponmocup Hunter 2.0 – The Sequel
- 2015 - LT: Creating your own CTI (in 3 minutes.. or 5 ☺)
- 2016 - Advanced Incident Detection and Threat Hunting using Sysmon (and Splunk)
- 2017 - LT: Sysmon FTW! ☺
- 2018 - Hunting and detecting APTs using Sysmon and PowerShell logging
- 2019 - DESKTOP-Group - Tracking a Persistent Threat Group (using Email Headers

Introduction
Setting Expectations

- More Q's than A's, sharing observations
  - I don't have all the answers (yet ☺)
- Call for Collaboration



c-apt-ure.blogspot.com/2022/01/who-is-desktop-group.html

Wednesday, January 26, 2022

Who is "DESKTOP-Group"?

This is just a preliminary post about my research of a threat actor (TA) or group (TG) that we have named "DESKTOP-Group". Other companies (Orange-CERT, Group-IB, SWIFT) have other names for this TA, but they are not yet publicly known or linked yet. *(I will update this post, as soon as more becomes public)*

We started tracking this TA's activity in early 2018, while analyzing the first malware laden attack mails during February 2018. For the next three years, we saw and analyzed 170 distinct attack mails (campaigns) from this TA, but during 2021 it became harder to link malware mails back to them with high confidence.

The first public presentation "*DESKTOP-Group – Tracking a Persistent Threat Group (using Email Headers)*" was at BotConf 2019. Slides (PDF) are available from my Github repo.

In 2020, I also presented about this TA at ReversingLabs #Reversing2020 online conference. A video (starts around 14:30m) and PDF slides are also available.

In 2019, I started sharing on Twitter about this TA, later starting to use the hashtag #DESKTOPgroup.

There is also a closed Google-group for research collaboration, mostly with people tracking or having access to emails or logs, related this TA's activity.

Malware samples and URLs have been shared and tagged on Abuse.ch Malware Bazaar or URLhaus.

Who is "DESKTOP-Group"?

This is just a preliminary post about my research of a threat actor (TA) or group (TG) that we have named "DESKTOP-Group". Other companies (Orange-CERT, Group-IB, SWIFT) have other names for this TA, but they are not yet publicly known or linked yet. *(I will update this post, as soon as more becomes public)*

We started tracking this TA's activity in early 2018, while analyzing the first malware laden attack mails during February 2018. For the next three years, we saw and analyzed 170 distinct attack mails (campaigns) from this TA, but during 2021 it became harder to link malware mails back to them with high confidence.

The first public presentation "*DESKTOP-Group – Tracking a Persistent Threat Group (using Email Headers)*" was at BotConf 2019. Slides (PDF) are available from my Github repo.

In 2020, I also presented about this TA at ReversingLabs #Reversing2020 online conference. A video (starts around 14:30m) and PDF slides are also available.

In 2019, I started sharing on Twitter about this TA, later starting to use the hashtag #DESKTOPgroup.

- 2018 – started tracking DESKTOP-Group @ SwissPost
- 2019 – first talk @ BotConf
- 2020 – second talk @ Reversing2020 (online)
- 2021 – Group-IB & Orange-CERT wrote Threat Report (yet unpublished)
- 2022 – SWIFT adds «DESKTOP-Group» alias to a TA they track & publish

Thanks for accepting my LT!!

- Twitter: @c_APT_ure
- Blog: http://c-apt-ure.blogspot.com/